



norman

Administrator's Guide

Norman Email Protection

version 5.70



Features

- Antivirus & Antispam
- Reports and system status
- WebAdmin and WebMonitor

Limited Warranty

The contents of this manual are for informational use only and are subject to change without notice. Neither Norman nor anyone else who has been involved in the creation or production of this manual assumes any responsibility or liability for any errors or inaccuracies that may occur in this manual, nor for any loss of anticipated profit or benefits, resulting from the use of this manual.

This manual is protected by copyright laws and international treaties. Your right to copy this manual is limited by copyright law and the terms of your software license agreement. As the software licensee, you may make a reasonable number of copies or printouts, provided they are for your own use. Making unauthorized copies, adaptations, compilations or derivative works for any type of distribution is prohibited and constitutes a punishable violation of the law.

Any references to names of actual companies, products, people and/or data used in screenshots are fictitious and are in no way intended to represent any real individual, company, product, event and/or data unless otherwise noted.

Norman and Norman Email Protection are trademarks of AVG Technologies. directQuarantine™, modus™, modusGate™ and Sequential Content Analyzer (SCA)™ are all trademarks of Vircom Inc. Windows, Windows Server 2003/2008/2012/2012 R2/2014, IIS, Internet Information Server, Windows Exchange Server, Active Directory, Windows SQL and Microsoft Outlook are either registered trademarks or trademarks of Microsoft® Corporation in the United States and/or other countries. Avira is a registered trademark of Avira Operations GmbH & Co. KG. Bitdefender Antivirus is a registered trademark of Bitdefender® Inc. All other products or services mentioned in this document are identified by the trademarks or service marks of their respective companies or organizations.

Norman Email Protection is based on the Professional Internet Mail Services product licensed from the University of Edinburgh.

Certain algorithms used in parts of this software are derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm.

Copyright (c) 2015 AVG Technologies

Norman Safeground AS (an AVG Technologies company)

Address: Strandveien 15, Lysaker, NORWAY

Postal: PO Box 43, 1324 Lysaker, NORWAY

For more information, visit our website at www.norman.com

Revised September 2015.

Table of Contents

Introduction.....	5	System	24
About this manual	5	Services	24
Product	5	Scanning order.....	27
Help and support.....	5	System databases	27
Contact support.....	5	Quarantine Reports.....	29
Related documents	5	License Key	31
Getting Started	6	Footer	31
Configuration requirements.....	6	Settings	32
Email Protection integration	6	Mail Delivery	34
Deployment scenarios	6	Global Aliases	34
System requirements	7	Agents	36
Database requirements	7	Proxy	37
Firewall configuration	7	Custom Errors.....	37
Exchange / Active Directory configuration.....	8	Preferences.....	37
Installing Email Protection	9	Security	38
Before you begin	9	Security overview	38
License key.....	9	Protocol Filter.....	38
Install Email Protection.....	10	Authentication.....	40
Overview	10	SMTP Security.....	40
Install Email Protection server	10	Mail Relay.....	42
Configuring routes	13	Block Scan Attack	42
Using the route wizard	13	Sender Reputation	43
Using the console: Connections	14	DNS Blacklists (DNSBL).....	45
Mail flow test	17	Connection Limits	46
Change the DNS record	17	Connections	47
Installing the web components separately	18	Trusted Address List.....	47
Modify the web configuration files	18	Encryption & Certificates.....	48
Configure the ODBC connection	19	Domain Keys.....	49
Folder permissions	21	Content Filters	52
Email Protection Administration	22	Overview of content filtering	52
The administration console	22	Virus.....	53
Navigating the console	22	Preference settings	53
Override functionality	23	Properties settings.....	55
		Domain virus controls	56
		User virus controls.....	57
		Phishing	58
		Overview	58
		Domain phishing controls.....	58
		User phishing controls	59

Table of Contents cont.

Spam.....	60	Troubleshooting.....	85
Preference settings	60	Basic Troubleshooting Guidelines	85
Properties settings.....	64	Connection problems with	
Domain spam controls.....	64	Exchange/AD	85
User spam controls	64	Mail delivery problems.....	87
Forbidden Attachments (F.A.)	66	Mail spool directories.....	88
General	66	Diagnosing problems using spool	
Forbidden Attachments.....	66	directory contents.....	89
Auto-Cleanup	67	Sieve script mistakenly captures test	
Postmaster	67	messages	89
Preference settings	67	Third-Party anti-virus blocks messages	
Options	67	and locks files	90
Alert Sender	68	Resolving backlogs in Holding and	
Alert Recipients	68	Domains folders	90
Domain attachment controls	69	Possible causes for email backlog.....	90
User attachment controls.....	69	Invirus buildup and/or server freezes	
Language Filter	69	at regular intervals	91
Performance	70	Web application issues	91
Domain language filter controls	70	Performance counters	92
User language filter controls.....	70	Appendices	93
Quarantine management	72	Appendix A: Web applications	93
Overview of features	72	WebMonitor	93
Console administration	72	System Health	93
User administration.....	74	Reporting	95
Logs	77	Message Audit.....	99
File Config	77	WebAdmin	101
Web.....	81	Appendix B: Formal command syntax.....	103
WebAdmin Privileges.....	81	Appendix C: Interacting with Exchange...	104
Domain WebAdmin controls	82	Appendix D: Processing Trusted and	
User WebAdmin controls.....	82	Blocked senders lists.....	105
Quarantine options	82	Glossary.....	106
Quarantine advanced	82		
Find.....	83		
Admin	83		
Quarantine	84		

Introduction

About this manual

This document is written for administrators to provide instructions for installing and configuring Email Protection Server and its web applications. It is assumed that the reader is familiar with Microsoft Windows operating system and Microsoft SQL servers.

Product

Norman Email Protection ASV is email relay with both anti-spam and anti-virus protection, including spam, phishing, virus and forbidden attachment blocking. Provides a full year of virus protection from Bitdefender® or Avira Antivirus.

Help and support

Contact support

If you have specific questions concerning the use of one of our products, please contact our support team.

- **Web:** www.norman.com
- **Email:** support@norman.com
- **Phone:** +47 67109700
- **Fax:** +47 67589940

Working hours are from 8 a.m. to 4 p.m., Monday to Friday.

Related documents

The documentation set for Email Protection can be found under the business section of:

- <http://www.norman.com>

Getting Started

Configuration requirements

Email Protection integration

Email Protection is a comprehensive email security gateway server that is compatible with Windows Server 2003, 2003 R2, 2008, 2008 R2, 2012, 2012R2. Windows Small Business Server 2008, 2011, and Virtual Machines (VM). It integrates with Microsoft Exchange, Lotus®Domino® and any standard SMTP server.

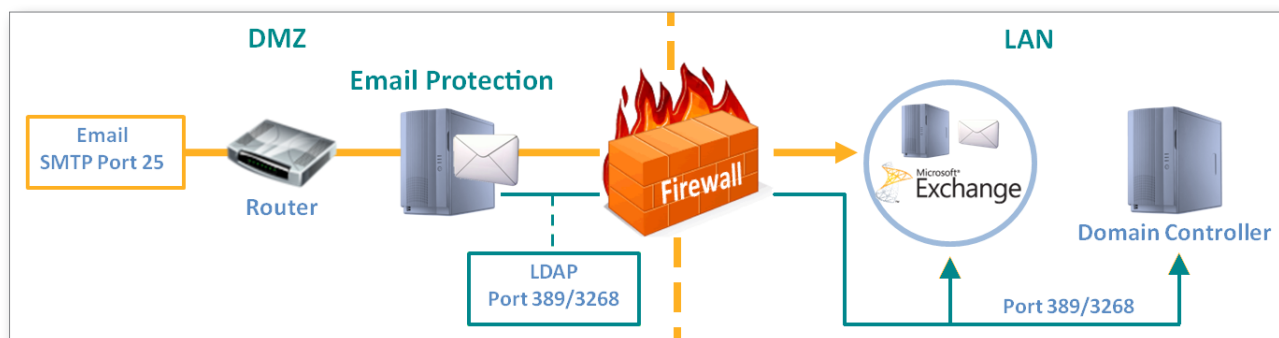
Because Email Protection was designed primarily to work with Microsoft Exchange, this section of the document will focus on its configuration with Exchange and Active Directory.

For deployment with Lotus Domino and other SMTP servers, please contact us. (Our contact information is available from our web pages www.norman.com.)

Deployment scenarios

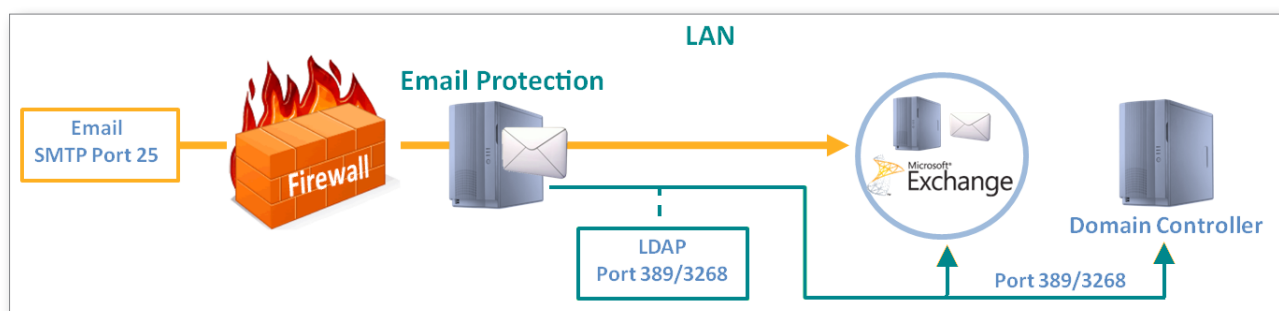
Scenario 1: Email Protection in the DMZ

With this method, Email Protection resides in the DMZ while the Exchange Server and other network resources are protected behind a firewall.



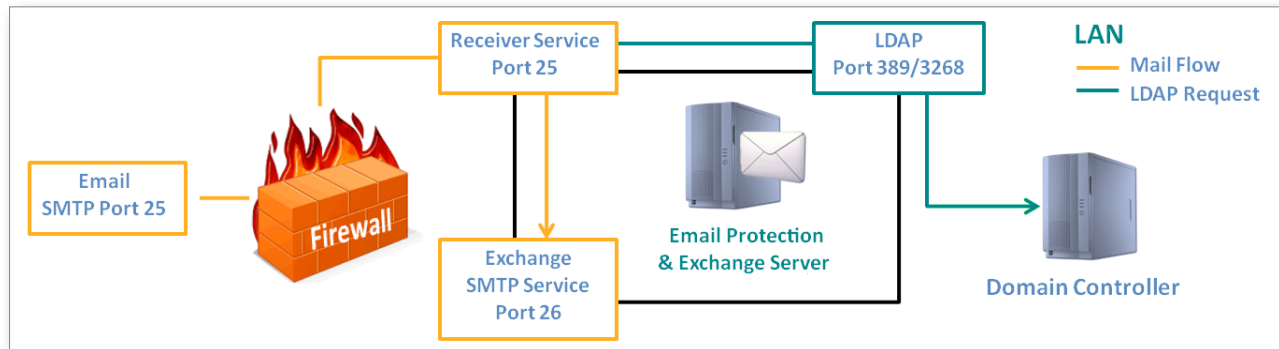
Scenario 2: Email Protection on the same subnet as Exchange

Here, the firewall provides Network Address Translation (NAT) or simple port filtering. After Email Protection is installed and configured, change the NAT rule to route email to Email Protection instead of directly to Exchange.



Scenario 3: Email Protection installed on the Exchange/SMB Server

Note that this setup is only recommended for use with a Small Business Server (SMB) or if email traffic is quite low. In this option, Email Protection must be configured to use SMTP Port 25, while the Exchange/SMB Server must be modified to use a different port for SMTP, e.g. 26.



Note that for Exchange 2013 changing the SMTP port should be done for both IPv4 and IPv6 when Email Protection is on the same server. The web components also get configured with https instead of http.

System requirements

For minimum recommended system requirements for Email Protection Server, please visit:

- http://www.norman.com/business/system_requirements

Database requirements

Email Protection requires databases for several of its features. If you do not have a database server installed, the Email Protection installation process includes Microsoft SQL Server 2005 Express with advanced services or Microsoft SQL Server 2014 Express LocalDB depending on the Windows version. Note that Full Text Indexing is required for some features.

Firewall configuration

If you plan to use a firewall, we recommend that you do not use Windows Firewall as it can cause problems with internal communication required by Email Protection. Instead, use a hardware firewall to protect your network from unauthorized external access.

Exchange / Active Directory configuration

Before you begin the Email Protection installation, verify the following settings on your Exchange / Active Directory server to ensure proper communication with Email Protection:

1. If using Exchange 2007 or 2010, it must be configured to accept email relay from Email Protection. Please use this Microsoft Technet article for configuration instructions:

<http://exchangeopedia.com/2007/01/exchange-server-2007-how-to-allow-relaying.html>

If using Exchange 2013, please refer to the article below:

<http://exchangeserverpro.com/exchange-2013-configure-smtp-relay-connector>

2. For Exchange 2007 or 2010: check if the Hub Transport or Edge Transport server role is installed. If either role exists, you must change these message throttling settings under Set-ReceiveConnector:
 - MaxInboundConnectionPercentagePerSource: Change the value to **20%**
 - MaxInboundConnectionPerSource: Change the value to **1000**

For complete details, see the following Microsoft KB articles:

[http://technet.microsoft.com/en-us/library/bb232205\(EXCHG.80\).aspx](http://technet.microsoft.com/en-us/library/bb232205(EXCHG.80).aspx) (ME 2007)

<http://technet.microsoft.com/en-us/library/bb232205.aspx#ReceiveConn> (ME 2010/2013)

3. You must have an account with **Read** permissions on the Active Directory/Global Catalog. This account and its password will be required when configuring Email Protection. Your Administrator account can be used, but creating a new account is recommended.

Follow the steps below to create a new account:

4. Log into the Domain Controller Server and go to **Start > Programs > Administrative Tools > Active Directory Users and Computers**.
5. Expand your domain name, right-click **Users** and select **New > User**.
6. Enter mgate in **First name**, copy it to **User logon name** and click **Next**.
7. Configure the **Password**, uncheck **User must change password at next logon**, check **Password never expires**, and click **Next** through the remaining screens to finish creating the user.
8. Click on **View > Advanced Features**.
9. Select **Security**, click on **Add** and enter mgate.
10. Under the **Allow** column, check **Read** and click **Apply**.

Installing Email Protection

Before you begin

Before beginning the installation, please review the following checklist of configuration requirements. These will ensure that Email Protection is fully functional after completing the install:

1. The server must be configured with a static IP and at least 1 DNS server address.

Go to **Local Area Connection settings > Properties > Internet Protocol (TCP/IP) > Properties**

2. The domain name must be specified in the Network Identification properties:

Go to **My Computer > Properties > Network Identification > Properties**

Confirm that the computer name appears in the **Computer name** field. Click on **More > Primary DNS suffix for this computer** and enter your domain name, e.g. `xyz.com`.

The server must be rebooted after this change.

If this information is missing, the Email Protection installer will automatically prompt you to enter it during the install process and launch a server reboot.

3. IIS 6.0 or above is already installed.
4. Both .NET Framework 4.0 Extended and .NET Framework 4.5 are installed.
5. Microsoft's built-in SMTP service is either disabled or set to manual (required to prevent conflicts on port 25).

Go to **Administrative Tools > Services** and set **Simplified Mail Transport Services** to **Stop**.

In the **Startup Type** dropdown menu, select either **Disabled** or **Manual**.

6. Verify that the following ports are open to allow for automatic spam, virus and license key updates and Web component access:
 - Port 80 for HTTP
 - Port 443 for HTTPS
 - Port 9000 (for directQuarantine, if required)

License key

Verify that you have your license key and copy/paste it to this screen (the characters are case-sensitive). If you do not yet have a key, you may contact Norman at sales@norman.com.

Install Email Protection

Overview

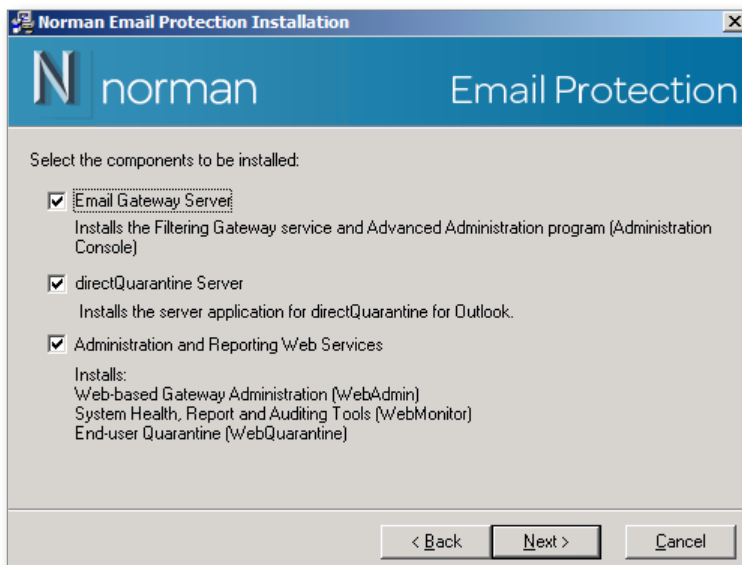
The installer includes the following three components:

1. The Email Gateway Server application, which provides the email gateway services and the Administration Console.
2. The directQuarantine Server application, which enables users to access and control their quarantined messages from within Outlook. This is an add-on program that is licensed separately; but is available for trial purposes and for fully licensed users.
3. Administration and Reporting Web Services, including WebQuarantine, WebMonitor and WebAdmin. These can optionally be installed on a separate web server.

Install Email Protection server

Follow the procedure below to install the Email Protection Server application:

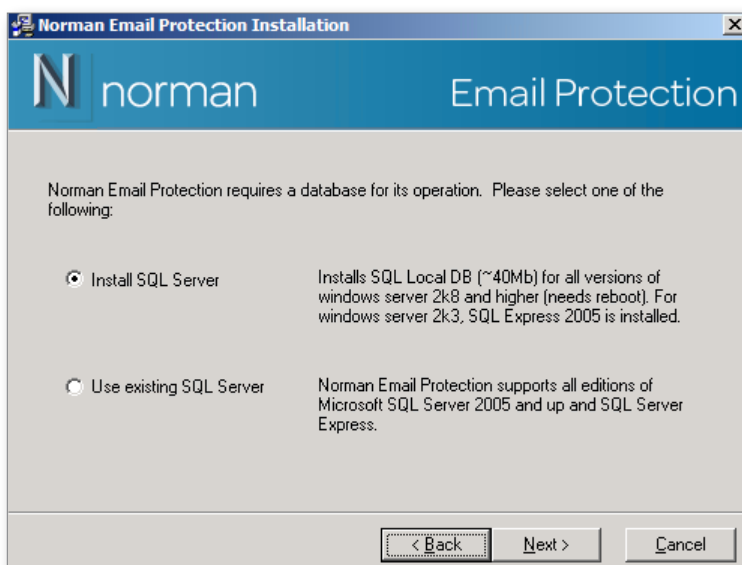
1. Log into the server using an Administrator account.
2. Click the NEP-5.##.###-ASV.EXE file to launch the installation.
3. Accept the licence agreement and click **Next** to enter your license key.
Click **Validate > Next**.
4. Choose a **Standard** or **Custom** install:
Select **Standard** to install all components on the local server, including the server application, directQuarantine and the web components.
See the **Custom** options in Step 5, otherwise continue at Step 6.
5. **Custom** allows you to select which components to install or disable, and provides advanced settings for database configuration.
If the web components are to be installed on a separate web server, select **Custom** and uncheck **Administration and Reporting Services**. See "Installing the web components separately" on page 18 for installation and configuration details.
If you plan to use directQuarantine, take note that it must be installed on the same server as Email Protection.



6. Click **Next** to verify the installation paths. Make any changes necessary and click **Next** to continue.

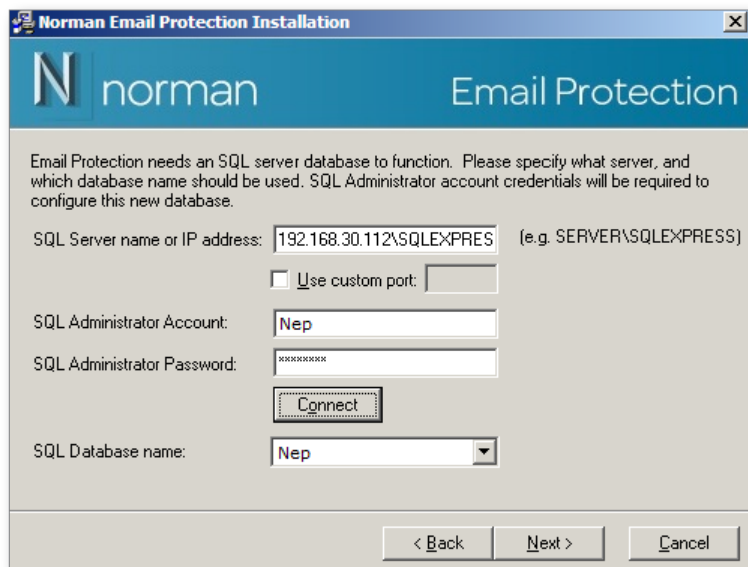
7. If you have a SQL Server on the local machine or network, select **Use existing SQL Server**. This option is automatically selected if a connection can be detected.

If you do not have a SQL Server, select **Install SQL Server**.



8. Click **Next** to enter the SQL Server connection details:

- **SQL Server name or IP:** if using SQL Express, include \sqlexpress after the IP or name. Do not enter spaces either before or after the backslash (\).
- **SQL Administrator Account:** enter the SA account name (or one with equivalent rights) and the Password.
- If you plan to use a new SQL database, select **New SQL Database**, input a name for the database or keep the default one.
- Else, if you want to use an existing database, select **Existing SQL Database**. If your SQL Server address and credentials are valid, the list of existing databases will be displayed so that you can select the desired one.



9. Click **Next** to launch the Email Protection installation and to create the database tables. This process will take a few minutes.

10. Click **OK** to start the Email Protection and IIS services.

At this point you might be prompted to enter a DNS Suffix: enter your domain name. If this step is necessary, Windows Server will require a reboot to register this change.

11. **Delivery failure notices:** if the DNS Suffix prompt does not appear, you will instead be asked to provide an email address for delivery failures. This must be a valid address on the primary email server: it is recommended to use your postmaster address.

12. If .NET Framework 4.0 is not detected on the server, you will be prompted to accept its download and install. This application is required for directQuarantine.

13. Clicking **Next** will launch both the Route Wizard and the What's Next HTML page containing configuration guidelines.

Configuring routes

Using the route wizard

After Email Protection is installed, the Route Wizard launches automatically to quickly and easily guide you through setting up the connection (or route) to your email server.

If you have multiple domains and/or email servers, or if your email server type is not specified in the drop-down list, it is recommended to configure the settings manually: click the Switch to Manual button to close the Route Wizard, and follow the directions in "Using the console: Connections" on page 14.

1. Enter your email **Domain name**, e.g. xyz.com.

2. Select the appropriate **Mail server type** from the dropdown list.

If your server type is not listed, select **SMTP, SMTP_VRFY**, or click the **Switch to Manual** button to use the Console Connections screens to configure your settings.

Please note the following important issues:

- The **SMTP** option cannot validate email recipients, therefore invalid addresses will be created in the user list and count against your user license. In addition, if alias email addresses are used, they will be added to the user list and total user count.
- **SMTP_VRFY** is supported by most email servers, but must only be used if the email server is protected by a firewall with no direct public access. Without a firewall, the list of valid user accounts can be easily obtained over the Internet. Alias email addresses are supported by SMTP_VRFY; they will not be counted against the user license.

3. Enter the **Mail server name or IP**.

4. The **SMTP Port** number automatically displays 25; change this only if you use a different number.

If your email server type is either SMTP or SMTP_VRFY, click Next and go to Step 9 for the remaining instructions.

If you had selected **Exchange** as the email server type, click **Next** and enter your **Active Directory/LDAP server** information.

5. If your email server type is either SMTP or SMTP_VRFY, enter a valid email address in the **Enter Email to Test** field and click **Test Route**.

- The system will attempt to connect to your email server and send a message to your address.
- You will receive feedback if there are any errors.
- Check your Inbox to confirm the message was received.

If you had selected **Exchange** as the email server type, click **Next** and enter your **Active Directory/LDAP server** information.

Enter the **AD root domain name**. This is the root or internal domain name configured on your Active Directory/LDAP server, e.g. domain.local.

6. Verify the **Port number**:

- If using Exchange 2003-2013, port **3268** is automatically configured for the Global Catalog: this provides access to the entire list of users' mailboxes. Selecting **Use TLS** will auto-reset the port to **3269**.
- If using Exchange 5.5, LDAP port **389** is set.
- You may optionally enter a custom port.

7. **User DN and Password:** enter the email address and password of the Administrator. The email address format is supported by both Active Directory and LDAP.

SBS Server Configuration

- You must enter an account using the format **@Windows domain** in the **User DN** field, if your Windows domain differs from your email domain name.

Example

your email domain name is company.com, but your Windows domain is company.local, you must enter admin@company.local as the User DN.

8. Enter a valid email address in the **Enter Email to Test** field and click **Test Route**.
 - The system will attempt to connect to your email server and send a message to your address.
 - You will receive feedback if there are any errors.
 - Check your Inbox to confirm the message was received.
9. Click **Next** to view the summary table and verify the information.
Click **Add** to enter other domains or email servers, if necessary.
To edit or change any information, use the Console's **Connection** settings.
Click **Finish** to close the wizard.

Using the console: Connections

Use the Email Protection Administration Console settings to set up routes:

1. Click on the Email Protection icon on your desktop to launch the Administration Console.
2. Click **Connections**, go to **Routes > Add Domain**.
3. Enter your email domain name in **Domain mask** and click **OK**, e.g., xyz.com.
 - Keep the **Route for incoming mail** setting: this is required when configuring Email Protection with a local (internal) email server.
 - **Route for outgoing mail** is only used if connecting to a email server that is external to your network.
4. Click **Add Route**: enter the IP or machine name of your email server.
Do not change the port number unless your email server uses a different SMTP port.
Click **OK** to display the **Properties** screen: the server's IP/name and port number are displayed in the **Route mail to host or IP address** and **Port** boxes.

5. **Automatically populate user list:** this is an authentication method that checks if the recipient address exists on the email server or not, and dynamically populates the **Users** list as email flows through Email Protection. All methods offer this security except **SMTP**. Choose one of the following:

SMTP: use this only if none of the other options apply. This is the least secure method as no authentication can be performed, thus invalid addresses will be created in the user list and count against your user license. Alias addresses are also unsupported and will be created as additional users.

- When selected, the adjoining boxes to the right should contain the same IP/hostname and port as those entered in Step 4.

SMTP_VRFY is supported by most email servers, but must only be used if the email server is protected by a firewall with no direct public access. Without a firewall, the list of valid user accounts can be easily obtained over the Internet.

- SMTP_VRFY is safe to use if only Email Protection can connect to the email server. Alias addresses are supported.
- When selected, the adjoining boxes to the right should contain the same IP/hostname and port as those entered in Step 4.

Exchange 2003-2013: address validation does occur and aliases are supported. Take note that distribution lists do count as mailboxes.

- In the right-hand boxes, enter the IP of the Active Directory (AD) Server if different from the Exchange server. Use port **3268** for access to the Global Catalog (the entire user list), or enter a custom port. You may optionally check **Use TLS**.

Lotus Domino: supports SMTP_VRFY so consider this option before trying to implement an LDAP-based solution.

- Depending on how aliases are configured on your email server, Email Protection may not be able to auto-detected them and count them as separate mailboxes.

OpenLDAP: is a generic LDAP auth mechanism that works with many email servers.

- Depending on how aliases are configured on your email server, Email Protection may not be able to auto-detected them and count them as separate mailboxes.
- In the right-hand boxes, enter the IP of the LDAP Server, if different from the email server. Use port **389** or enter a custom port. You may optionally check **Use TLS**.

Disabled is an advanced option, used to lock the user list and prevent invalid addresses from being dynamically created. This is typically used if Active Directory/LDAP cannot be used for mailbox validation.

- The user list must be populated in advance, either manually or by using SMTP until the list is complete.

Exchange 5.5: using this option requires configuring custom attributes to be used with LDAP and is therefore not recommended. It is preferable to use **SMTP_VRFY** instead, which must be configured on the Exchange server:

- Open the Registry Editor on the Exchange 5.5 Server
- Go to **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MSExchange\Parameters**
- Right-click and select **New > DWORD value**
- Enter **EnableVRFY**
- Double-click **EnableVRFY > Value data** and enter **0x1**.

6. **Authentication Requests:** this is required to validate the login credentials to access the WebQuarantine and WebMonitor programs. This setting must be consistent with what was selected for **Automatically populate user list**. The servername/IP and port fields must also match the settings above:
 - Use **SMTP Auth** if either SMTP or SMTP_VRFY was selected above
 - Use **Exchange 2003-2013** if selected above.
 - If OpenLDAP was selected above, you may choose either **OpenLDAP** or **SMTP Auth**.
 - **POP3** is used only in rare circumstances if SMTP Auth is not supported by your email server. If selected, you must also enable **Strip domain name from Authentication requests**.
7. If you had selected **Exchange** or **OpenLDAP** in Step 5, complete the **LDAP Identification** section:
Base DN: enter your email domain name using this format: DC=domain,DC=com.

Example

The email domain is xyz.com, enter DC=xyz,DC=com

- **User DN and Password:** enter the email address and password of the Administrator or mgate user (see "Exchange / Active Directory configuration" on page 8). This format is supported by both AD and LDAP.
 - It is recommended to use the mgate account because its access to user information is restricted and therefore more secure.
 - If the mgate user has not been created yet, enter the Administrator's information temporarily, and then change it in the console's Connection screen afterward.

SBS Server Configuration

- You must enter an account using the format **@Windows domain** in the **User DN** field, if your Windows domain differs from your email domain name.

Example

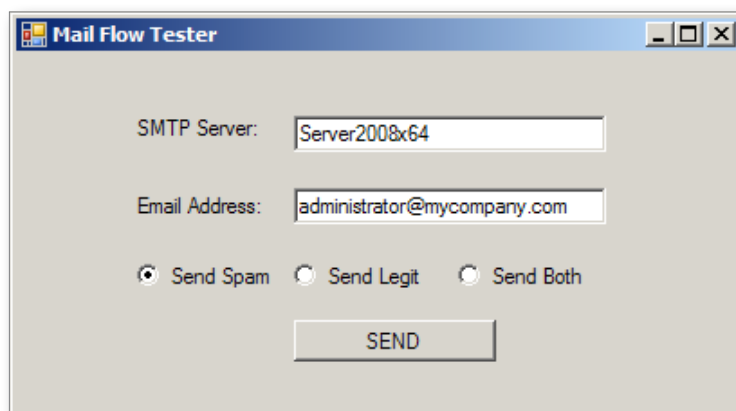
your email domain name is **company.com**, but your Windows domain is **company.local**, you must enter **admin@company.local** as the User DN.

8. Click the **Test Route** button and enter a valid email address. This test will confirm whether or not Email Protection can connect to the email server and send a legitimate test message.
Check your Inbox to confirm the message arrived.
9. Repeat the above steps, if required, for each additional domain or email server.

Mail flow test

After verifying the route configuration, you can optionally run this automated email flow test to ensure the system is working properly:

1. After the installation is completed, open the Email Protection Administration Console to [System > Services](#) to verify that all services are running.
 - The most important services required for basic functionality are: SMTPRS, SMTPDS, MODUSADM and MODUSCAN.
2. Locate the Email Flow Diagnostic Tool on the desktop and click to open the program.
3. Verify that the SMTP server displays the Email Protection server name, and enter your email address to perform the test.



4. Select to test a legitimate email, spam or both, and click **Send**
 - Check your Inbox in Outlook to verify that you received the legitimate test email.
 - On the Email Protection console, open the [Quarantine](#) tab and verify that the spam test message appears in the list (if the console Quarantine screen was already open, you might need to click the [Refresh](#) button to see the message).

5. The email flow test can be re-run at any time.

If using a Email Protection blockade or redundant setup, you can test other Email Protection server(s) by entering their server names.

Change the DNS record

Once your connections are tested and working, the next step is to change your DNS records.

- On the DNS Server, modify the MX (Mail Exchange) record so that your email domain points to the Email Protection server instead of the Exchange.
- Create an A or Host record that maps the new Email Protection MX to the Gate server's IP address
- Since new MX records can take anywhere from 12 to 48 hours to propagate, only remove the email server's MX after Email Protection's MX has been propagated. Do this to hide your email server from public view: when spammers see multiple MX's for the same domain, they often bypass the primary (Email Protection's) and target the secondary (the email server).
- If you wish to check whether your MX record change has been propagated, try using our Email Security Grader tool at www.emailsecuritygrader.com and enter your domain name.

Installing the web components separately

The following instructions apply only if you plan to install the web components on a separate server from Email Protection. You will need a copy of your Email Protection installation file and the Email Protection license key.

1. Log into the server using an Administrator account.
2. Copy the Email Protection xxx.exe file to this server and click to launch the installation.
3. Enter the same license key you used on the Email Protection server and click **Validate > Next**.

The license key must match that of the Email Protection server or the web components will not work.

4. Select Custom and ensure that only **Administration and Reporting Services** are selected in the check box options.
5. Verify the installation path and click **Next**. Note that all web files will be installed together.
Click **Next** to complete the installation.
6. Follow the instructions below to ensure that each of the web components communicates properly with Email Protection.

Modify the web configuration files

Each of the following web components will require manual changes to their configuration files to ensure proper communication with Email Protection server.

WebQuarantine

1. Open Windows Explorer to the ...**Norman\Web\Quarantine** directory.
2. Locate the **WebMailSvr.ini** file and open it with Notepad.
3. Locate the **host=xxx.xxx.xxx.xxx** and verify that it shows the IP address of the local (Web) server.
4. Locate the **ModusGateServer=xxx.xxx.xxx.xxx** address and change this to the IP of the Email Protection server
The POP3 and IMAP address default to the localhost; leave these as is (they are not used)
5. Locate **DomainName=machine_name.mydomain.com**: change this to match the primary domain as it appears on the Email Protection Console
6. **Save** the changes.

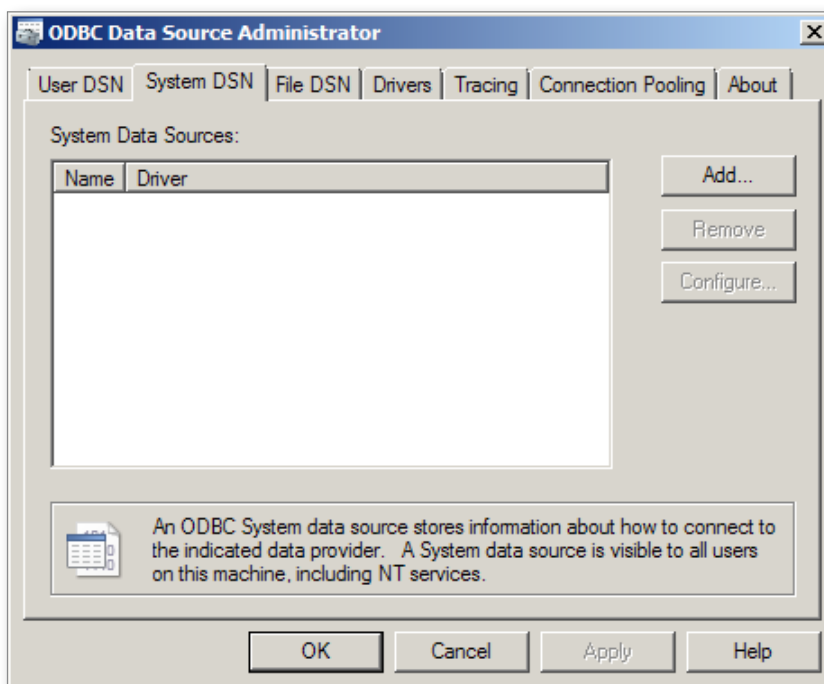
WebAdmin

1. In Windows Explorer, go to the ...**Norman\Web\WebAdmin\Root** directory.
2. Locate the **web.config** file and open it with Notepad.
3. Locate `<add key="Site" value="" />` and enter Email Protection's IP address between the empty quotes.
4. Open **Administrative Tools > Services** and restart the WEBMAILSVR service.
5. Restart the IIS service to register the collective changes for all the web components.

Configure the ODBC connection

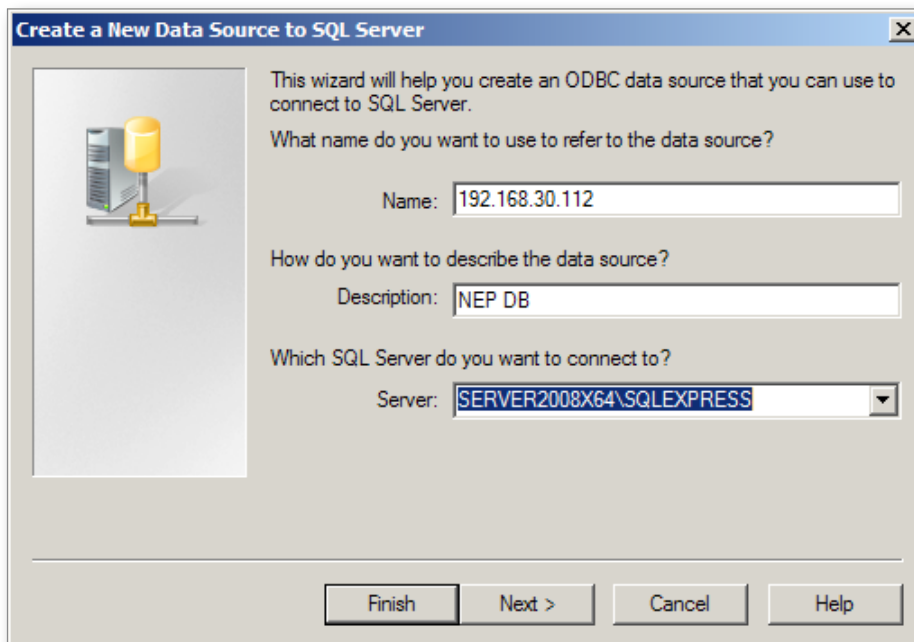
To access database resources, you must manually configure an ODBC connection on the web server:

1. On the server that now houses the web components, go to **Start > Administrative Tools > Data Sources (ODBC)**.
2. Select **System DSN > Add**.

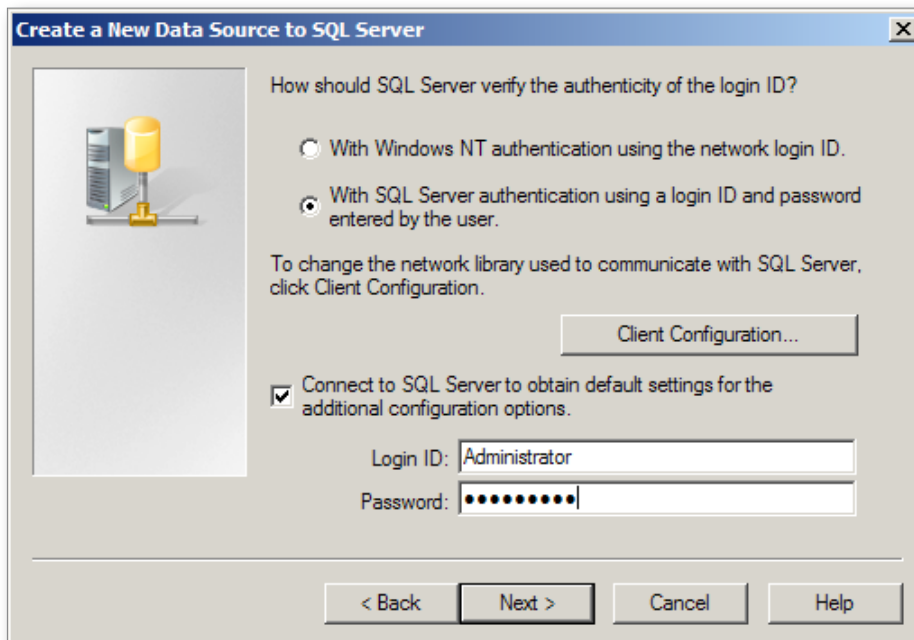


3. Select the driver that matches your database type and click **Finish**.
 - For SQL Server 2005 Express: select **SQL Native Client**
 - For all other SQL versions, select **SQL Server**.

4. Enter a name for the connection and the SQL Server address (can be the IP address or hostname).
 - For SQL Express, enter servername\squlexpress. Click **Next**.



5. Select **SQL Server authentication** and enter your login credentials, e.g. the sa account and password. Click **Next**.



6. Select the **modus** database and click **Next**.
7. Click **Finish** and **Test Data Source** to confirm a successful connection.

Folder permissions

The following folder permissions configuration applies to both a single and dual-server setup:

Open Windows Explorer and locate the ...\\Norman\\Web directory.

- Right-Click on Web, select **Properties > Security > Edit**.
- Click **Add > Advanced > Find Now**.
- Select the following accounts from the list: IUSR, ASPNET and Network Service and click **OK**.
- Enable **Modify** permissions for each account and click **OK**.
- Be sure to replace the permissions on all child objects (the exact steps vary with different OS versions).

Restart the WEBMAILSVR and IIS services to register the above changes.

All programs can be accessed using the following URL format: http://127.0.0.1/[app name] (e.g. http://127.0.0.1/webmonitor), You can also enter the machine's specific IP or custom website name if you created the site manually.

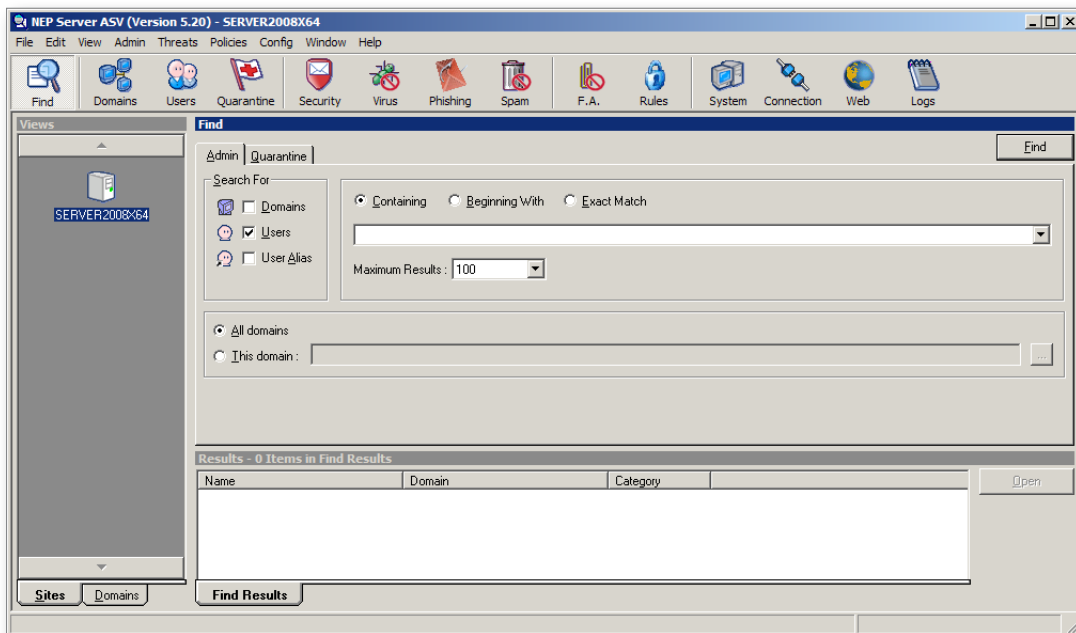
Email Protection Administration

The administration console

The Administration Console is designed to provide a high level of flexibility and control over the Email Protection server configuration. It gives you the option to set system-level parameters that can be applied to all users, or to customize particular settings for select domains and/or users who require special email handling rules.

Navigating the console

To navigate through Email Protection, click on the Toolbar buttons at the top of the console. You will then find a series of tabs or panels within each screen.



Views

The **Sites View** displays the machine name where Email Protection is installed.

The **Domains View** lists the domains for which Email Protection is filtering and/or relaying mail.

- The list of domains (if multiple) is created dynamically once the Connections or routes have been configured and email begins to flow through Email Protection.
- Double-clicking a domain name in the Domain view will display the properties panels for that domain. (Note that clicking the **Domains** button in the toolbar will produce the same behavior.)

Users

- The list of users is also created dynamically once email begins to flow through Email Protection.
- Click the **Users** button in the toolbar: the results window will display all usernames in a given domain.
If there are multiple domains, click the domain name to see the list of users for that domain.
- Double-clicking a username in the results window will display the properties panels for that user.

The Users list will not populate dynamically if, in the Connections screen, you set Automatically populate user list to Disabled. (This is an advanced option used for special configuration requirements, and/or to prevent automatic cleanup of unused mailboxes during the regular synchronization process.)

Override functionality

To support customization, override settings are available in the domain and user properties for the following features: alias addresses, footers (or disclaimers), audit logging, and filter controls (where applicable), including language preferences for the Quarantine Report and the WebQuarantine interface.

Server Level

- Configuration changes made at the server level are propagated to all domains and users.
- Users and domains are able to override settings unless Forced options are enabled (i.e. for scan functions).

Domain Level

- Configuration changes made at the domain level affect all users within that domain.
- Domain-level settings will override the server settings if permission to override was granted.

User Level

- Configuration changes affect only the individual user.
- User-level changes override the server and domain settings if permission to override was granted.

In general, Email Protection checks for and applies settings in this order: 1) User, 2) Domain, and 3) Server.

Exceptions to this rule do exist and will be highlighted where applicable.

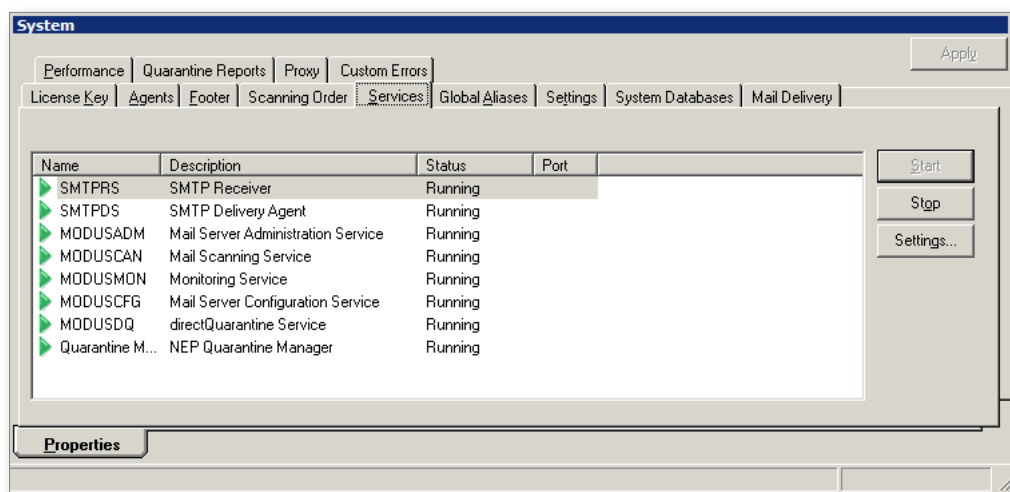
System

This following sections in this document describe the configuration options and recommended settings for each of the Toolbar panels, beginning with the core System settings.

Services

From this panel, you can start, stop and configure the Email Protection services:

- Click on a service to select it
- Click on **Start**, **Stop** or **Settings**
- If **Settings** is not available, the configuration cannot be modified for this service



These services can also be started and stopped in the **Administrative Tools > Services** panel, and are set to start automatically.

SMTPRS

The SMTP Receiver Service is responsible for performing the following actions:

- Receiving all incoming email from the Internet.
- Applying all security settings on incoming messages and either accepting or blocking them according to your rules.
- Performing mailbox validation to ensure that the message recipient has a valid account on your system. When the address is invalid, the message is rejected, thus reducing the load on the email server.

Click **Settings** to configure the **Transmission** and **Submission** ports:

Transmission: the standard port is 25. This is the port used by external email servers to communicate with your server. Do not change this port unless you do port mapping via a proxy server or firewall.

Submission: this port is used when local users are configured to send outbound email through Email Protection to the Internet. The standard port used for this purpose is 587.

- You can configure your Exchange or other email server to use port 587 to route outbound email to Email Protection for scanning prior to delivery to the destination addresses.
- Another option is to configure the users' email client settings to use port 587 as the SMTP server port. However, this requires making a change on each user's machine.

SMTPDS

The SMTP Delivery Service is responsible for the following actions:

- Relaying email to your email server for local delivery to the mailboxes.
- Handling email for delivery to external (non-local) email addresses.
- Processing only the messages that have passed security and content checking.

Click **Settings** to configure an IP address for outbound messages, if necessary. This is only used if you use separate IPs for incoming and outgoing email traffic.

MODUSCAN

The Email Protection Scanning Service does the following:

- Handles messages after they have been verified and accepted by the SMTPRS/security checks.
- Runs attachment, spam scanning and/or virus scanning, where applicable.
- When spam and/or dangerous content is found, it handles messages according to your preferences, e.g. quarantine, delete or 'tag and pass.'
- If messages are considered legitimate, they are passed to SMTPDS for delivery.

MODUSADM

This is the server administration service, responsible for automatic updates of the spam and/or virus engines, filter definitions and the quarantine database. It is also responsible for a number of internal functions.

MODUSMON

This service is used by the WebMonitor application to provide updated server statistics and maintain the monitoring database.

MODUSDQ

This is the directQuarantine server service, which provides end users with a live view of their quarantined messages in Outlook and the content controls.

WEBMAILSVR

This service controls the WebQuarantine server service, if installed on the Email Protection server. When the web components are installed on a separate machine, the service appears stopped (this is normal behavior).

Summary: message processing sequence

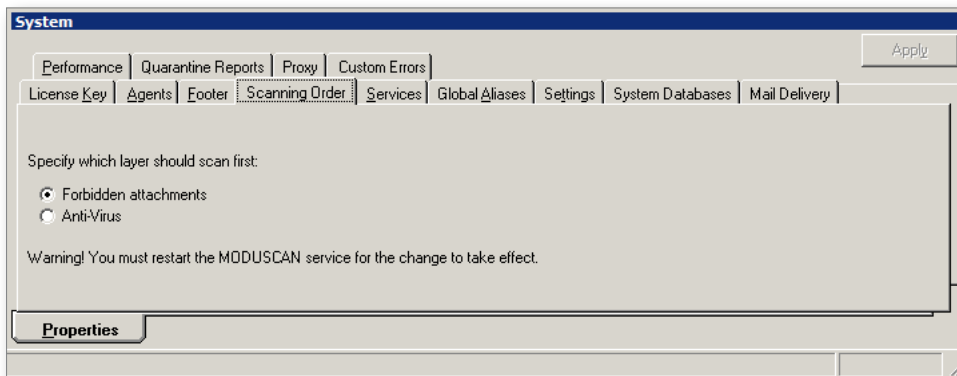
This is a very brief overview of how Email Protection processes messages:

1. A sending email server opens a connection to Email Protection.
2. The SMTPRS service responds, requesting the sending server's identification and the message header details.
3. SMTPRS then applies all configured security checks to validate the supplied information. If the message fails any security criteria, or if the recipient address does not exist on the local system, the connection is rejected and closed.
4. Message transmission begins after passing all security criteria.
5. The MODUSCAN service then begins scanning the message (according to applicable options).
6. If the message fails the scan, it is treated according to the handling rules.
7. If the message is clean, it is then passed to the SMTPDS service for delivery/relay to the email server.

Scanning order

Email Protection is configured to scan messages for **Forbidden Attachments** prior to scanning the content for **Viruses**. This order is designed to reduce processing load on the server and increase the speed of message handling.

You may optionally reverse this order, but you must stop and restart the MODUSCAN service to register this change.

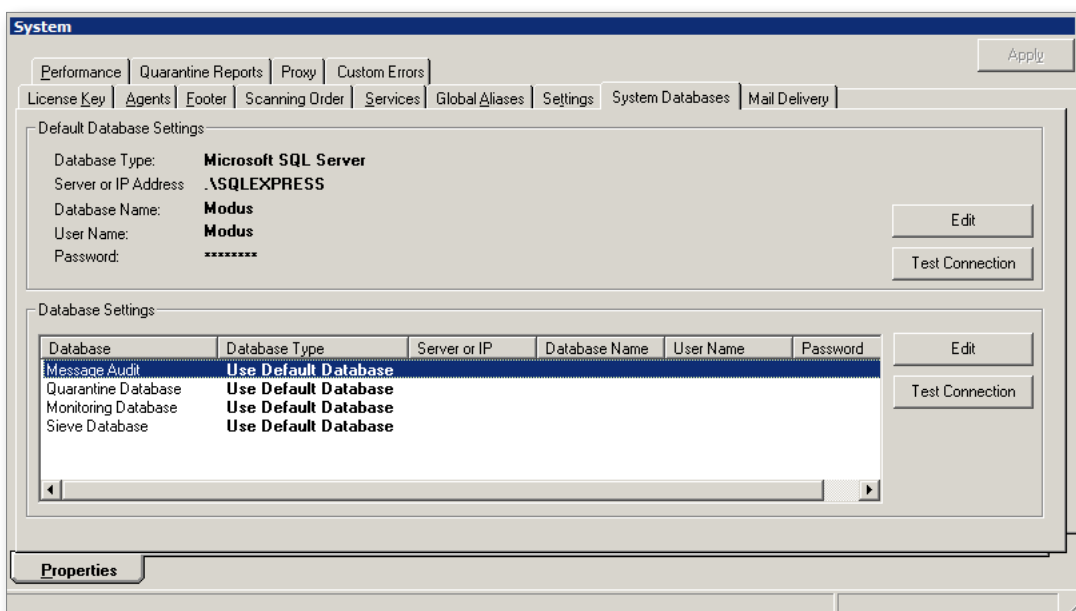


System databases

Multiple databases are configured automatically during the Email Protection installation. These include the Message Audit, Quarantine, Monitoring and Sieve (containing spam definitions, trusted and blocked senders lists, and any custom filters you might create). All are stored in the "Default" location, however settings can be modified for individual databases.

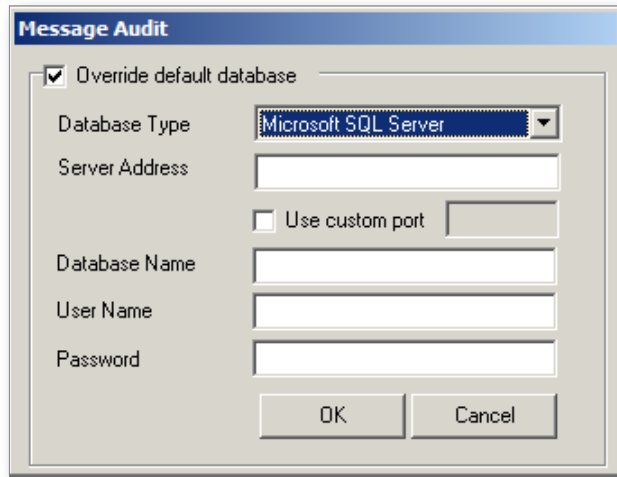
EXAMPLE

If you have a large number of mailboxes on your system (e.g., 500 or more), you should create a separate Quarantine database to ensure better performance.



If you wish to modify a particular database, follow the steps below:

1. Select the database name and click **Edit**.
2. Enable **Override default database**, if applicable. (Note that the Default database can also be modified and has its own Edit controls.)



3. Use the dropdown menu to select the **Database Type**. The menu will display different options depending on the database format supported.

PostgreSQL is considered legacy platform and is no longer recommended. In addition, if you plan to use the Greylisting feature in the Security settings, the Default database must be SQL: Postgres is not supported.

4. Enter the **Server Address**: use either the IP or server hostname.
5. Enable **Use custom port** if necessary. Email Protection dynamically determines the port for SQL Server, but change it manually if it is incorrect.
6. Enter the new **Database Name**.
7. Complete the **User Name** and **Password** fields. If this account does not yet exist on the database server, the necessary access rights will be configured automatically.
8. Click **OK** to create the new database structure.

If you wish to move or copy data stored on the 'old' database, this must be done manually using the SQL Server import/export controls.

9. Optional: click **Test Connection**.

This option can be used at any time to verify that Email Protection is able to communicate with the database server

Extended Database

If you use a Blockade configuration of two or more Email Protection servers, we provide the Extended Database structure to store Users' properties.

The database script can be found in the Email Protection program files:
...\\Norman\\Norman Email Protection\\DBStructures\\SQL Server\\ExtendedDB.

Quarantine Reports

Email Protection provides the option to send quarantine reports to your users. The report is a summary digest that is emailed on a scheduled basis.

Links within the report allow users to release or delete spam, add sender addresses to their trusted or blocked lists, and in some cases release forbidden attachments (with special permission).

If a user releases a message containing a forbidden attachment, it is scanned for viruses (where applicable). Consequently, the message could be quarantined again, in which case it cannot be released through the report.

Reports will not be generated in the following cases: a) for people who have disabled reporting, either at the domain or user levels and b) when no new spam, viruses or attachments have been caught since the previous report was generated.

To configure quarantine reports for the entire system:

1. Select **Enable reporting**.

The screenshot shows the 'System' configuration window with the 'Quarantine Reports' tab selected. The 'Enable reporting' checkbox is checked. Below it, 'Generate reports every' is set to 3 hours, on 'Every day'. A 'Generate Now' button is present. The 'From' time is 8:00 and 'To' is 16:00. The 'Last Report Time' is Friday, February 22, 2013 2:00:00 AM. The 'WebQuarantine URL' is http://localhost/quarantine, with a 'Test Url' button. There are four checkboxes: 'Allow one-click release' (checked), 'Add a link to permit Users to disable Quarantine reports' (checked), 'Users must login to change blocked / trusted lists and quarantine report settings' (unchecked), and 'Allow users to access their report settings' (checked). At the bottom, there are dropdowns for 'System Report' (Default) and 'System Theme' (Default), a 'Display Name' field, and a 'From Email' field containing postmaster@server2008x64.norman. A 'Set Report Content' button is next to the 'System Report' dropdown. A 'Properties' tab is visible at the bottom left.

2. Enable **Generate reports every** and set the desired frequency. Note that the minimum hourly schedule is 3 hours: this limit reduces the potential performance impact on the server.
3. If WebQuarantine is installed on the Email Protection server, the **WebQuarantine URL** should display <http://127.0.0.1/quarantine>.

If your server is configured with both IPv4 and IPv6 IP formats, be sure to use 127.0.0.1 ('localhost') in the URL. Or, if WebQuarantine is installed in a separate server, replace 'localhost' with the web server's IP.

Or, if you prefer, enter the web address according to your configuration in IIS, e.g., <http://www.mycompany.com/quarantine>.

4. Click **Test** to ensure that a "URL test successful" message appears in a web browser on the Email Protection server. The test must succeed for the quarantine reports to function properly.
5. Select from the following access control functions:
 - Allow one-click release:** allows users to release their quarantined email using the links within the Quarantine Report.
 - Add a link to permit Users to disable Quarantine Reports:** allows users to opt out of receiving the Quarantine Report.
 - To enable this function, you must first go to the **Web** section of the console **> Allowed User Properties > Edit**, enable **Reporting Frequency** and click **Apply**.
 - Users must login to change blocked/trusted lists and quarantine report settings:** this forces users to login to WebQuarantine before making any changes to these settings
 - Allow users to access their report settings:** creates a link in the Quarantine Report that provides users with direct access to their settings in WebQuarantine.
6. You may change the following report format settings, if desired:
 - System Report:** is the master layout for the Quarantine Report, controlling how the messages are displayed. You may optionally create a custom report with your own display preferences, which can then be selected from the dropdown menu.
 - System Theme:** you may optionally customize the colors, fonts, logos, etc., used in the Quarantine Report. Use this setting to select a custom theme.
 - Display Name:** enter the email address to be displayed in the **From:** field in Quarantine Report messages.
 - From Email:** enter the email address to be used when sending the reports. By default, the postmaster address is used.
7. **Set Report Content:** these settings determine what message details are included in each user's Quarantine Reports. The default settings provide the maximum amount of information.

A note about the **spam probability levels:** this feature can be used as a filter to display only the messages that may have been quarantined in error (i.e., False Positives). It is recommended to select the **Medium** and **Low** probabilities for this purpose.

 - Messages labelled **High** probability can safely be disabled for most people.

Optional: You can allow users to set their own report content preferences by enabling permission:

 - In the Console, go to **Web > Privileges > Allowed User Properties > Edit**, enable **Reporting Content** and click **Apply**.
 - Users will then have access to these settings by logging into WebQuarantine, and can make any desired adjustments.

Domain Quarantine Report controls

Override settings for the Quarantine Report language and content controls are also available in the Domain properties in the Console:

- In the toolbar, click **Domains >** select the domain name **> Reporting**. Enable **Override server default settings**, and make any necessary adjustments.
- In the **Domain** tab, enable **Override** to select a language for the Quarantine Report. The default is English.

User Quarantine Report controls

Override settings for the Quarantine Report language and content controls are also available in the User properties in the Console:

- In the toolbar, click **Users >** select the user name > **Reporting**. Enable **Override domain default settings**, and make any necessary adjustments.
- In the **General** tab, enable **Override** to select a language for the Quarantine Report. The default is English.

License Key

This panel provides important information about your license key, including the expiry date, your current build and patch versions, and the number of licensed users.

Validate: any license changes authorized by Norman Safeground, such as product renewal, increasing users, purchasing add-on programs, etc., are updated via your license key and validated automatically by system. **Validate** can be used to manually update changes, but it is not necessary to do so.

Browse: use this function to locate and select your license key text file if doing a manual validation.

The **Users** section displays the current number of licensed users and how many seats remain available. An automatic process runs daily to synchronize the user names between Email Protection and your authentication server (such as Active Directory/LDAP), and to remove any invalid addresses or those that are no longer active on the authentication server.

In some cases, administrators flag certain mailboxes as inactive on the authentication server but must continue to keep and/or receive email for them. These addresses may be automatically removed by Email Protection's synchronization process. To prevent their removal from Email Protection, do the following:

- In the Console, go to **Users >** select the username that must be kept
- In the **General properties** tab, enable **Keep this user permanently > Apply**.
- The **Disable Account** option is only available if the user account on the authentication server has been disabled.

Synchronize Now: can be used to manually synchronize the user names.

Threshold Warning: Email Protection issues a warning notice when the number of users approaches 95% of the limit allowed by your license. You may adjust this threshold to receive these warnings earlier (using a lower percentage, e.g., 80%) or later (using a higher percentage, e.g., 98%).

Example

if the maximum number of mailboxes is 500 and the threshold is set to 95%, a warning message appears when there are 475 users on your system.

Footer

From this panel, you can enter footer or disclaimer text to be inserted at the end of every outbound message sent from the email server.

To use this feature, you must configure your email server to route outbound messages (i.e., to non-local email addresses) through Email Protection.

Domain footer controls

Footer settings can be customized per domain:

- Go to **Domains > domain name > Footer**. Enable **Override default message settings** and **Append this message to the end of each outgoing message**.
- Enter your text, select **Format** and click **Apply**.

User footer controls

Footer settings can also be customized per user:

- Go to **Users > user name > Footer**. Enable **Override Domain Default Settings** and **Append this message to the end of each outgoing message**.
- Enter your text, select **Format** and click **Apply**.

Settings

This panel contains general server settings, such as the directories for the email spool and system logs.

Mail Spool Directory: this is the location of the message spool or queue.

The spool can optionally be moved to another drive on the Email Protection server, but placing it on a network shared drive is not recommended. If you move the spool, you must enter the new directory here, and stop/restart all Email Protection services.

The spool must not be placed on a separate server from Email Protection.

System Log Directory: this is the location of the system logs, such as operational and error logs.

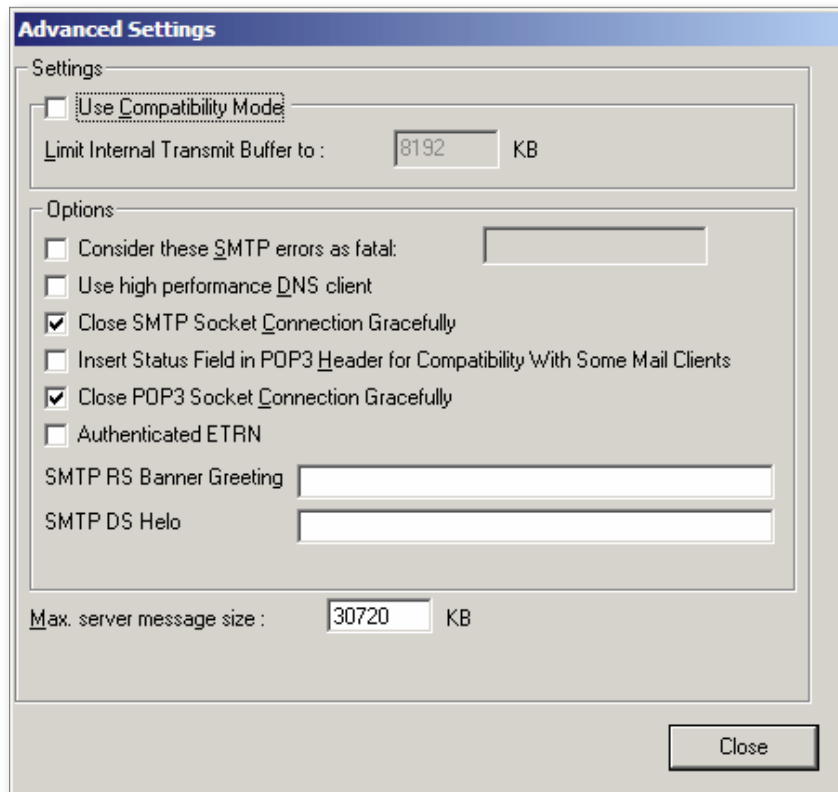
This directory can be moved to another drive, including a network shared drive. If you move the log directory, you must enter the new location here and stop/restart all Email Protection services.

Language: used to select the language for the Quarantine Reports. The default is English.

The language can be customized per domain (see "Domain Quarantine Report controls" on page 30) or per user (see "User Quarantine Report controls" on page 31).

Send delivery failure notices to this email address: displays the email address entered during installation, if enabled. You may change this address at any time.

Advanced options:



The image shows a screenshot of the 'Advanced Settings' dialog box. It has a title bar 'Advanced Settings' and a 'Close' button at the bottom right. The dialog is divided into two main sections: 'Settings' and 'Options'. In the 'Settings' section, there is a checkbox for 'Use Compatibility Mode' which is unchecked. Below it is a text field 'Limit Internal Transmit Buffer to:' with the value '8192' and the unit 'KB'. In the 'Options' section, there are several checkboxes: 'Consider these SMTP errors as fatal:' (unchecked), 'Use high performance DNS client' (unchecked), 'Close SMTP Socket Connection Gracefully' (checked), 'Insert Status Field in POP3 Header for Compatibility With Some Mail Clients' (unchecked), 'Close POP3 Socket Connection Gracefully' (checked), and 'Authenticated ETRN' (unchecked). Below these are two text fields: 'SMTP RS Banner Greeting' and 'SMTP DS Helo'. At the bottom of the dialog, there is a text field 'Max. server message size:' with the value '30720' and the unit 'KB'.

Use Compatibility Mode: Do not enable - this setting does not apply to Email Protection.

Consider these SMTP errors as fatal: when enabled, you can specify a list of numerical error codes, separated by a comma (,). When Email Protection encounters one of these errors from a another server, it will bounce the message immediately without attempting to resend it.

Use high performance DNS client: if the default DNS client is too slow when performing reverse DNS look-ups, an alternate (high performance) DNS client can be used instead.

Close SMTP Socket Connection Gracefully: use this option if Email Protection experiences problems with SMTP sockets that remain in an indefinite WAIT state. This setting will enable Email Protection to close the sockets.

Authenticated ETRN: when enabled, an SMTP client must first be authenticated through the AUTH command with a valid mailbox name and password before using the ETRN command.

Reject messages with empty bodies: certain types of spam messages are sent with empty bodies and are therefore missing the final single dot that signals the end of transmission. Using this setting blocks such messages and prevents processing issues on Email Protection.

SMTPRS Banner Greeting: use this option to create a custom banner greeting, if desired. This greeting is seen by external email servers when they initiate a connection to Email Protection.

SMTPDS HELO: this setting enables you to modify how your domain name appears in the HELO line when sending messages to another server.

Max server message size: this value sets the maximum message size (in KB) that the server will accept. A value of '0' denotes no message size limit.

Mail Delivery

This is the message delivery schedule: a list of time intervals when Email Protection attempts to resend email that could not be delivered successfully. Time is measured from the moment message delivery fails to when the next attempt is made.

Messages are kept in the Email Protection spool or queue while delivery is retried at each interval listed. If the final time is reached, the message is deemed undeliverable and returned to the sender. Times marked with an envelope icon indicate when a notification is generated, informing the sender that the message has not yet reached its destination.

The retry frequency can be modified by adding or removing intervals. This is especially useful if/when your email server goes offline for any reason. The final time can be increased (e.g., from 2 days to 4 or more) to ensure that messages to your users remain stored on Email Protection until the email server is back online. The maximum retry delivery time is 22 days.

- Click **Add** to enter a new time interval to the list: enter the required Days, Hours and/or Minutes.
- Select an interval and click **Remove** to delete it from the list.
- Use **Send Warning/No Warning** to enable/disable sender notifications at a specific time.

If an unusually large number of messages begin queuing for a particular domain, you can attempt to force delivery using one of two methods:

- **Force automatic retry for these domains:** Click **Domain List**, enter the domain name(s) and set a **Retry count**: this will be the total number of retry attempts.
- **Enter the domain names for immediately delivery:** enter the domain name(s) or a wildcard in the text box and click **Deliver Now**.

Neither of these methods guarantee delivery. Serious connection issues can occur on the receiving end that prevent successful delivery.

Global Aliases

This feature allows you to create global aliases for your system, such that email sent to one address can be redirected another. For example, you want email addressed to domainA.com to be redirected to domainB.com.

When not to use Global Aliases

You should note that this is a legacy feature that has been kept to support certain older systems that require it. Alias settings exist in both the Domain and User properties, which are recommended for use instead. See "Domain alias controls" on page 35 and "User alias controls" on page 36.

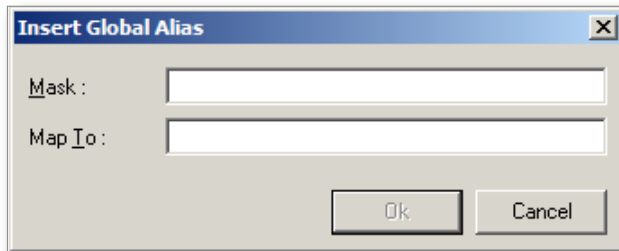
Do not use this feature if any of the following situations apply to you:

- You plan to enable Quarantine Reports for your users.
- You have aliases already configured on your email server, and your routes are configured to use either SMTP_VRFY or Exchange/Active Directory. These aliases are usually detected and added to the users' properties automatically.

Configuring Global Aliases

Should you need to use this feature, follow the directions below:

1. Click **Insert** to add an alias.



EXAMPLE

You want email addressed to domainA.com to be redirected to domainB.com.

2. Enter the alias address in **Mask**, i.e., domainA.com from the example above.
 - Wildcards are accepted, e.g., *@domainA.com.
3. Enter the destination address in **Map To**, i.e., domainB.com from the example above and click **OK**.
 - This must be an actual address on the system: it cannot be an alias.
 - Wildcards are accepted, e.g., *@domainB.com.
4. Use the **Up** and **Down** buttons to set the priority.
 - Aliases are processed in the order listed.
 - Wildcards must be placed at the end of the list.
5. Optional: use **Import** to populate the list using a text file.
 - You must enter a single alias/destination pair per line using the format, mask address: map to address. Enter a space before and after the colon (:).

Example

domainA.com: domainB.com

6. Use the **Find** button to search the list. Wildcards are supported.

Domain alias controls

Domain alias names can be configured in the console:

- In the toolbar, click **Domains > select domain name > Aliases**.
- Click **Add**, and enter the alias name.
- Aliases are used when you want email addressed to domainA.com to be redirected to domainB.com. The 'redirect to' addresses must exist on your system.

User alias controls

User alias names can be configured in the console:

- In the toolbar, click **Users > select user name > Aliases**.
- Click **Add**, and enter the alias name.
- Aliases are used when you want email addressed to userA@domain.com to be redirected to userB@domain.com. The 'redirect to' addresses must exist on your system.
- Depending on your alias configuration in Exchange/Active Directory, user aliases are usually detected automatically and dynamically created in the Console.

Agents

An **Agent** calls an external program, such as a script or batch file, that runs every time the server receives a message. It can be used to redirect, copy (archive) or to delete messages.

If your Email Protection version supports the use of sieve scripts, it is recommended that they be used instead of agents, especially when archiving messages. Agents process messages before content filters are applied, thus messages containing malware will also be archived.

To create an agent, follow the directions below. The example given will archive all inbound and outbound messages that pass through Email Protection:

1. In the Agent text box, type the name of the batch file or program to be run, followed by %m %r
 - The %m directive copies the message file
 - The %r directive copies the header envelope
 - Be sure to enter the full path to the file name with quotation marks ("")

EXAMPLE

```
"C:\Progra~1\Norman\Norman Email Protection\ARCHIVEMAIL.BAT" %m %r
```

Click **Apply**.

2. Open Notepad to create your batch file. Click **Save As** and enter the filename from Step 1 (e.g., archive-mail.bat).

Save the file to a folder in the system path, e.g., "C:\Progra~1\Norman\Norman Email Protection\..."

3. Enter the following text:

```
@ECHO OFF
FIND /I "@domain.com" %2 > nul
IF %errorlevel% == 0 COPY %1 C:\AnyDestinationFolder\
```

Email Protection only supports the ability to direct messages to a specified folder, not a mailbox

Proxy

If Email Protection is installed on a network that is configured to access the Internet through a proxy server, you must enter the proxy server information in this panel. This is required to access the spam engine and anti-virus updates.

Click **Use a proxy server** and enter the host or IP address and the port of the proxy server.

Custom Errors

From this panel, you can create custom error messages for each of the **Error types** listed in the dropdown menu. If nothing is entered in these fields, the default error messages are used.

Custom error messages will only appear in your own error logs. External servers receive only default errors.

Preferences

These settings enable you to configure how long to cache SMTP authentication information for Email Protection. This allows validated senders to maintain open connections to the server for the time you set before having to re-authenticate.

Cache Size: specify the number of entries to keep in cache.

Cache Entry lifetime: specify the number of seconds to keep the cache entry.

Keep SMTP Connection Alive For: specify the number of seconds to keep the connection open. This option can also be used to terminate abandoned or hung SMTP requests.

Security

Security overview

Email Protection's security tools provide full flexibility to prevent spam attacks and security breaches on your email system. Every security feature was designed to help businesses maintain system integrity.

All security settings affect the system as a whole: they cannot be modified per domain or per user. Please follow the guidelines and proceed with caution when modifying the settings. If you have any questions or need further details, please do not hesitate to contact our support team at support@norman.com.

Using address lists (mask lists)

In most of the following features where address lists are created, you can use wildcards and other formatting to accelerate the process of entering IP addresses, host names and email addresses. Supported formats include:

*	The wildcard (*) denotes inclusion, i.e. use all variations of the entry. EXAMPLE: To block all yahoo.com addresses, enter *@yahoo.com This format is accepted in all lists, except where specified.
!	The exclamation mark (!) denotes an exclusion, i.e. use all entries except this one. This format is accepted in most lists, except where specified.
/xx	CIDR (slash) notation or netmask. This format is supported by all features where IP addresses are entered, to denote and include subnet masks. EXAMPLE: 192.168.42.23/24

The order of entries in the lists is important, as Email Protection applies rules from the top of the list downwards. To set the priority of a specific entry, use the **Up** or **Down** buttons.

Most features allow you to create and store text-based lists elsewhere on the server and to specify the file location in the feature settings, without having to manually recreate the list in the console. However, doing so may cause performance issues, particularly if lists are quite long. It is therefore recommended to import list contents into the console to speed up response times. Lists may be updated and reimported at any time, overwriting the previous lists with the updated entries.

Protocol Filter

The protocol filter allows you to block email messages based on header content. This filter comes enabled and pre-populated with several known header formats that have been used in past attempts to bypass various security measures.

How the filter works

There are two parts of an email - the envelope and the header - that contain the sender, recipient and other address information. The envelope is deleted when the message is delivered successfully. The header is part of the message (it can be viewed in the email client). In the envelope, the sender field is mailfrom and the recipient is 'rcptto'. The equivalent fields in the header are 'from' and 'to', respectively.

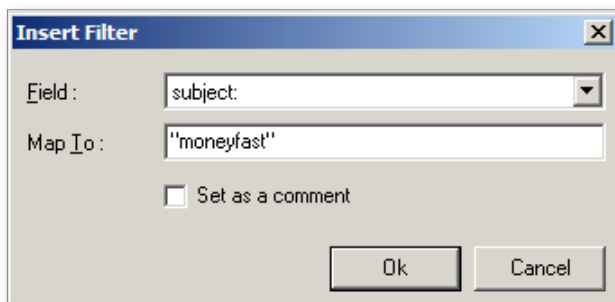
The protocol filter is used by specifying a list of text strings that correspond to the envelope/header content to be rejected. All incoming messages are checked against the filter list, and a message gets rejected when a matching entry is found.

Because the envelope and header addresses can differ, it is good practice to a) use wildcards, and b) create duplicate strings for the mailfrom/from and rcptto/to pairs.

The filter file name must be SPAMFLT0.TXT and must be located in your Email Protection directory

To add a new filter string:

1. Click **Insert** to add a new string



2. In the **Field** box, select the element to be filtered.
3. In the **Map To** box, enter the string you want to block. Use wildcards (*) to block variants of the string.

Example

You want to block subjects like "Make money fast".

Enter `*money fast*`

This will capture messages containing random characters before and after the subject (a trick to evade filters).

4. Click **OK** to save the entry and repeat the process to create as many entries as necessary.
5. Optional: **Set as a comment** inserts a pound sign (#) to tell the filter to ignore that particular string.
6. Use **Edit** to change an existing filter.
7. Use the **Up** and **Down** buttons to change the priority: filters are applied in order from top to bottom.
8. Stop and restart the SMTPRS service to register any changes.

Authentication

This panel provides several SMTP authentication mechanisms.

Force authentication for these IP addresses:

- Enable this setting to specify a list of IP addresses required to use SMTP authentication when relaying email.
- It forces users to authenticate prior to sending email through Email Protection. Users must have SMTP Auth enabled on their email clients. Without authentication, message transmission will be blocked.

Do not advertise SMTP Auth (for these IPs):

- SMTP Auth is normally 'advertised' or displayed as an available authentication method when the EHLO command is issued in the message header. Spammers can potentially hack users' accounts by collecting passwords that are transmitted to the server in clear text via PLAIN or AUTH LOGIN mechanisms.
- It is recommended to enable this feature and to enter *. *. *. * in the adjoining **IP Address** list.
- It is also used to support email clients that force the use of SMTP Auth when they see SMTP Auth as advertised.

Force encrypted transmission of authentication credentials

- Enabling this setting will block the transmission of clear-text credentials (it won't actually do the encryption).
- It supports PCI and other compliance regulations that require encrypted transmission of users' login credentials when sending email.

Allow transmission of clear-text credentials from these addresses only

- If the encryption setting is enabled, the local machine's IP and the local IP range (127.0.0.0/24) -used by the web applications - are automatically added to the exemption list to allow users to login (note that these addresses can be removed manually).
- The WebQuarantine program does not support the use of encrypted logins.

When authenticating via SMTP AUTH, the authentication is only valid for the current SMTP session. Once the session is closed, by default the same user will not be automatically authenticated for subsequent attempts; his credentials will be rechecked during the next login. This eliminates the possibility of spoofing.

SMTP Security

This panel provides several options for verifying the address format used when sending mail.

Force usage of fully qualified addresses in SMTP commands

- The system will reject messages that do not use a proper email address format (e.g. user@domain.com) in either the email from: or rcpt to: fields
- This feature helps to block mass-mailed messages sent to unspecified addresses or <Undisclosed Recipient>.

Reject malformed addresses

- Used to reject messages where addresses are not contained within angled brackets (<>) in either the email from: or rcpt to: fields, e.g., <user@domain.com>.
- Standardized email clients such as Outlook and Outlook Express support this format.

Validate Sender Addresses

- Performs a reverse DNS check on the sender's address.
- Recommendation: set **Cache Size** to 9000, and **Keep in Cache** to 240

Enable Bounce Address Tag Validation (BATV)

BATV checks for backscatter spam (or misdirected bounces). Backscatter occurs when a email server receives spam and legitimate email, and sends bounced messages to the recipient. However, with spam, the original MAIL FROM field usually contains a legitimate (but forged) email address. During a spam wave, a email server may generate bounces to the forged MAIL FROM addresses, thus redirecting the email to the legitimate email address who is the real target of the spammer. This could result in the server's IP address being placed on DNS blacklists.

When BATV is enabled, SMTPDS adds an encrypted tag to the email FROM field of all outgoing messages. If a bounce returns without a tag, then we know it did not originate from Email Protection. The message is either rejected or quarantined (depending on your settings).

Additionally:

- Validation is performed after the RCPT TO command so that messages are blocked before their content is transferred
- If an address is invalid, Email Protection processes it as a permanent failure by returning a 550 response to the SMTP command containing the address.
- If a message is identified as a bounce and not BATV validated, SMTPRS will return a 550.5.7.5 error code:

BATV uses the following format: Tag Type = Tag Value = Loc-core

E.g.: prvs=13266C8ED1=John@domain.com

The Tag Type is "prvs" (private simple signature)

The Tag Value is 13266C8ED1 and is unique for every message sent

The Loc-core is the mailfrom address John@domain.com

Apply BATV checking when the message contains matching subject tags from this list

- Click **Subject Tags** to enter a list of commonly used subject tags (e.g., out of office) to reduce the likelihood of false-positives.
- Use only one entry per line.
- Do not use commas (,) to separate entries as they are forbidden characters.

Disable BATV for these IP addresses

Click **IP Addresses** to enter IP addresses or IP classes for which BATV will not be used.

When enabled, Email Protection sets a default grace period of 7 days. During this time, no messages are filtered using BATV to prevent improper handling of older messages. BATV filtering begins when the grace period ends.

For more information about BATV, see:

<http://tools.ietf.org/html/draft-levine-smtp-batv-01>

Mail Relay

This feature allows you to specify which IP addresses or domains are allowed to relay email through your server, preventing your server from being used as an open relay.

Mail Server Cloaking

- This hides the email server from public view when relaying email for a defined route.
- Email Protection becomes the **public-view** server.

Accept email for relay...from these hosts

- Enter the IP addresses and/or domain names that are allowed to send email through the server (i.e. to external addresses).
- The localhost address (127.0.0.1) and the IPs corresponding to your configured routes are automatically added to this list.
- When adding addresses, accepted formats are: 10.10.10.10, 10.10.10.*, 10.10.10.0/16, and domain.com.

Block Scan Attack

This feature allows you to limit the number of recipients per incoming message. This effectively prevents spammers from sending messages with an unusually high number of recipients. You can also prevent dictionary spam attacks by slowing them down or blocking them.

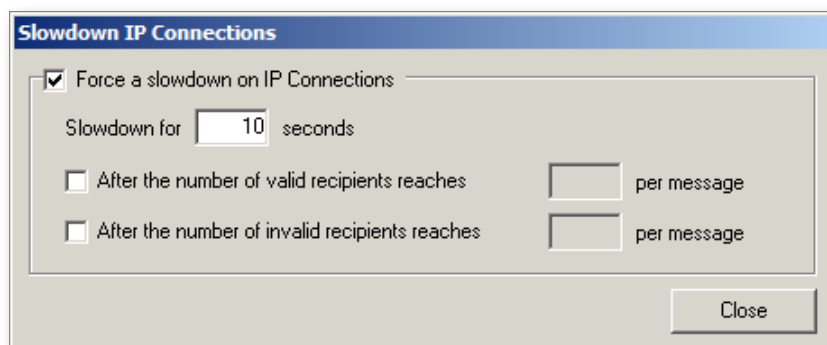
- To exclude specific IP addresses from this limit, go to **Security > Trusted Address List > SMTP Security Trusted Address > Trusted Address**, and enter the IP addresses.

Limit the Maximum Number of Valid Recipients

- Allows you to limit the number of recipients per message accepted by SMTP.
- The message will be rejected if the number of recipients exceeds this limit.

Slowdown the IP Connections

- When the set message threshold is reached, a slowdown is enforced between each subsequent message from the sending IP.
- Enter the number of seconds for which the connection will be slowed.
- Enter the number of valid and invalid recipients per message, after which the connection will be slowed.



Block IP Addresses

- Used to block IP connections that violate the threshold.
- Enter the number of minutes for which the connection will be blocked.
- Enter the number of valid and invalid recipients per message, after which the connection will be blocked.
- To prevent a dictionary spam attack, use the Block IP option and enter a low number (3-5) for invalid recipients.

The Slowdown the IP Connections and Block IP Addresses settings should not be used at the same time. The 'Slowdown' settings will override and disable the 'Block' settings.

Caching

- Set the maximum cache size.
- Enter the maximum number of IP addresses that will be kept by the system. When the maximum is reached, the oldest IP entry in the cache will be removed.

Maximum Entry Life Time

- Enter the lifetime of an entry in the cache.
- When the maximum is reached, the oldest IP entry in the cache will be removed.

Sender Reputation

Sender Reputation System (SRS)

This is the DNSBL, or DNSBL Blacklist service.

SRS classifies email based upon who is sending the message rather than its contents. Upon establishing a connection to the SMTP receiver service, a DNS query is made to the DNSBL with the IP address of the computer connecting to the service. If the IP address is found in the blacklist, that computer is considered to be a spammer. The connection can either be dropped immediately or the message from that sender can be quarantined.

This blacklist differs from other DNSBLs in that it is highly dynamic. It is updated every few minutes, based on who is sending the most spam to our honeypots. Similarly, if someone spams our honeypots accidentally, they will automatically be removed from the list a few hours after they stop spamming.

Sender Validation: Greylisting

Basic Mode (default): Email Protection sends a temporary error to the sender after the DATA command in the SMTP protocol exchange.

- Upon receipt of a temporary error, a valid SMTP-compliant mail server will resend mail. By contrast, spam-sending zombies are unlikely to resend mail.
- Basic Mode provides a strong defense against text and image spam. In fact, because the temporary error is sent before the body of the message is received, this mode does not discriminate if the message contains text or image spam.

Norman Extended Mode (recommended): Email Protection sends a temporary error to the sender after the END of DATA command CRLF.CRLF.

Extended Mode is designed to protect against spam and is intended to work in conjunction with the SCA engine. While the SCA engine is very effective at blocking image spam, the speed with which spammers create variants of their images has required us to increase our spam blocking efforts.

How it works

A spam tactic is to send 1000's of copies of a single image spam, containing randomly modified versions of the image, during a short period of time. Spammers do this by taking advantage of a delay between the time the new image spam variant is detected and the time it takes to create a new signature for the image. In as little as a few seconds, before new signatures can be created, the spammer can count on at least a small percentage of the variant image spam making their way to the users' inboxes.

The extended mode adds protection by reducing the spammer's window of opportunity for sending variants of image spam:

- When the first image spam is received, a signature is created for the message and cached.
- The message is not accepted. Instead, a temporary error is returned to the sender. This blocks a significant number of image spam because few spammers will resend.
- If the message is re-sent, a signature is created for this message.
- The signatures of the first and second messages are compared. Valid senders always resend the same message; therefore the signatures will be identical and the message will be delivered. By contrast, a spammer is unlikely to resend the exact same message. In the event that a spammer sends a second message (albeit a different one), Email Protection will respond to it in the same manner as it did for the first and the message will be cached. Assuming an identical message is never resent within the cache time frame (i.e. 4 hours by default), the sender's IP address will be added to the blocked senders list.

Differences between Basic and Extended Modes

Basic Mode (how greylisting is normally implemented) cannot block messages where the spammer resends it using the same MAIL FROM: and RCPT TO: pair.

Extended Mode will block messages if there is any modification to the content. It will not be activated if the spammer resends the exact same message.

Because Extended Mode is only activated when the message body contains an image, this causes fewer delivery problems for local users.

Regardless of the mode used, the following are not subject to greylisting:

- Trusted IP Addresses (Trusted Address List, Authenticated via SMTP_AUTH.)
- Senders whose domain has a SPF record but only if SPF Support is enabled (see [SPF Support below](#).)
- Sender's IP address if found during a [whitelist](#) lookup but only if the feature is enabled (see [Perform a lookup for SMTP host in the Real-Time Whitelist servers](#).)

Greylisting database information

- To support greylisting, the default database (see [System > System Databases](#)) must be configured to use SQL Server. No other database formats can be used.
- Greylisting database records are automatically expired after 8 hours.

Log Entries

Greylisting will generate two types of log entries in the OPR (Operations) log:

1. "Message from <Sender's IP> was temporarily rejected because of greylisting policies."
 - This is the most common log entry, indicating that the sender was given a temporary error.
2. "Message from <Sender's IP> was rejected because of greylisting policies."
 - This log entry only occurs when message is not re-sent within the default 4-hour time-frame. Failure to re-send within a 4-hour limit results in blacklisting the IP address for a 4-hour period.

Sender Validation: SPF support

Sender Policy Framework helps detect email sent with faked or forged sender addresses. SPF support only works for those domains that put SPF definitions in their DNS.

For more information about SPF, see <http://www.openspf.net/>.

Perform a look up for the SMTP host in the DNS

- Enables Reverse DNS lookup: this allows you to check if the IP of the sender's server resolves to the given domain name.
- This option is processor-intensive: you should monitor system performance when using it.

Reject Connection Immediately On Lookup Failure: when enabled, messages are rejected when the reverse lookup fails. This setting works together with the **Lookup Timeout:** the connection can also be rejected when the DNS lookup reaches the specified timeout limit.

Postpone the rejection until authentication: Email Protection looks for an SMTP AUTH connection before performing the reverse lookup.

Do not reject connection (Accept all hosts): the results of the DNS lookup are logged, but the message is processed whether the lookup fails or not.

To exclude IP addresses from Reverse DNS, add them to the **Security > Trusted Address List > SMTP Security Trusted Address** settings.

Perform a lookup for SMTP host in the Real-time Whitelist Servers

- Enable any of the specified Real-time Whitelist servers available for use with Email Protection.
- If the sender's server information is approved by the Whitelist servers, it bypasses the Email Protection connection settings. However, the content is still subject to spam and virus scanning (if applicable).

DNS Blacklists (DNSBL)

DNSBL (or DNS-based Blackhole lists or Blacklists) are 3rd party databases that contain lists of IP addresses belonging to known spam sources. Email Protection checks incoming email against these blacklists, and if a sending server's address is found, its email will be blocked.

This feature is disabled by default, and the following options must be enabled by clicking **Perform a look up for the SMTP host in DNSBL**.

Select the DNSBL servers where the look up will be made

- Click on **DNSBL Servers** to enter the IP address or DNS server name for the DNSBL you want to use.
- Certain lists can be aggressive and may cause legitimate email to be blocked from entering your email system.

Select the host IP's that will be excluded from the look up

- **IP Exclusion:** enter the IP addresses that will bypass the DNSBL lookup.
- If you must allow email from a DNSBL-listed server, add its IP to the exclusion list to ensure email delivery.
 - Alternately, add the IP address to **Security > Trusted Address List > SMTP Security Trusted Address**.

Reject connection immediately if the host is blacklisted: DNSBL runs at the beginning of the connection and blocks any server found on the list(s). This option is recommended to optimize speed.

- If disabled, the connection will only be severed after the RCPT TO command.

Perform DNSBL check after mailbox authentication: Email Protection waits until the sender's email address can be validated through SMTP Auth before determining whether to block the server or not.

- This benefits users who may have legitimate accounts on your system but whose sending IP addresses are listed on a DNSBL. With this setting, Email Protection first verifies the address and accepts and processes email only if it is legitimate; otherwise, the connection will be closed.

Caching: Allows you to specify how many RLB lookups will be kept in cache and for how long.

Possible DNSBL connection issues

Using DNSBLs may affect system performance, therefore you should monitor the server when using this feature.

We have no affiliation with any DNSBL nor does it have control over their content and availability. If an DNSBL goes down or is no longer in service, email flow will slow down or may be halted entirely (as no DNS resolution can occur). We are never warned of issues and, as such, cannot notify its clients.

To troubleshoot a possible DNSBL problem:

1. Open the **DNSBL Server** list, click **Export**, and copy and save your list to a text file.
2. Click **Remove** to delete all addresses from the list. Click **Close** and **Apply**.
3. Go to **System > Services**. Stop and restart the SMTPRS service.
4. From a command prompt, telnet to port 25 to check the banner response (it should be immediate).
5. Using your saved DNSBL text file, re-enter each address, one at a time, into the Email Protection list. Click **Apply**, and perform the telnet test after each entry.
6. When the problem DNSBL has been identified (i.e. banner response is not immediate), remove that entry and stop/start SMTPRS.

Connection Limits

This feature allows you to limit the number of simultaneous SMTP connections allowed from a single IP- which is unlimited by default. This option enables you to control performance as it limits the number of users allowed to use your system at a given time.

Total number of connections allowed for this server

- Used to specify the total number of simultaneous SMTP connections allowed on your server at one time.
- The default is set to 500.

Total number of simultaneous connections allowed from the same IP

- Used to specify the number of simultaneous connections allowed from one IP address.
- The default is set to 10.

Maximum connection rate allowed for this server

- Used to limit the total number of connections allowed per second.
- The default is set to 50.

Maximum simultaneous connection rate allowed from same IP

- Used to limit the number of new connections allowed per second, per IP.
- The default is set to 10.

Connections

These settings allow you to block connections from specific IP addresses. If a user has been identified for abusive email practices, he/she can be prohibited from using the email system.

Reject all incoming email from these hosts

- Enter the addresses to be prohibited from sending email to your server. Both IP addresses and domain names can be entered here.

Reject all incoming email from these addresses

- You can use this list to enter specific email addresses to be blocked from sending email to your server.

Trusted Address List

These settings allow you to enter the IP addresses that are considered “trusted” or allowed by your email server.

SMTP Security Trusted Address:

Mail sent from the IP addresses entered here bypass the following list of security checks. This affects both inbound and outbound messages, therefore you should limit the list to internal and well-known sources only.

- Block Scan Attack
- Reverse DNS
- Real-Time Blacklist
- Banned IP Addresses
- Connection Limits
- SPF
- Greylisting
- Protocol Filter

IP addresses entered here must also exist in the Mail Relay > Accept mail for relay from these hosts.

Scanning Trusted Address:

This setting is available only to the Email Protection versions that provide spam scanning. It is used to allow email from local IPs to bypass all spam scanning on outgoing email bound for the Internet. Virus and attachment scanning, if available, will not be bypassed.

Incoming Internet email will continue to be scanned according to your configuration.

IP addresses entered here must also exist in the Mail Relay > Accept mail for relay from these hosts.

Encryption & Certificates

Use this panel to configure encryption and certificate settings to add an extra level of protection to your email system.

Encrypt Message Transmission / Incoming transmission

Using certificates will ensure that your incoming email transmission connections are protected against unauthorized access. Different certificates can be used per domain or IP to ensure unique encryption signatures and improve security. Note that this method protects the communication channel between servers, but not the message content.

To use this feature, you must generate a self-sign certificate or purchase an SSL certificate.

For more information on purchasing a certificate, visit company websites such as www.thawte.com, www.verisign.com or www.entrust.com.

Use the following directions to configure Email Protection to use certificates:

1. Purchase and install the server certificate(s) according to the issuer's instructions.

Certificates MUST be installed in the default local computer account or Email Protection cannot use them.

2. In the Email Protection console, go to **Encrypt Message Transmission > Incoming Transmission > Use certificate**. Select the certificate name and click **Apply**.
3. To assign different certificates to different IPs, click **Advanced Certificate Setup > Add**. Enter the IP, select the certificate name to be assigned and click **OK**.

Repeat this process for each IP/certificate assignment required.

4. In **Select encryption protocol**, choose the appropriate format from **TLS 1.0**, **TLS 1.1** or **TLS 1.2**.
5. Select **Enable SMTP Encryption** and click **Apply**.
6. Stop and restart both the SMTPDS and SMTPRS services under **System > Services**.

Encrypt Message Transmission / Outgoing transmission

This option enables modus to use TLS encryption for outgoing SMTP connections without having to configure a certificate on the Email Protection server. If the remote (receiving) SMTP server supports TLS connections, that server will use its own certificate to handle the encryption. If not supported, modus reverts to sending the message in plain text.

To enable it, select **Enable SMTP Encryption > Use opportunistic encryption for SMTP transmission...** and click **Apply**.

When encryption enabled, force incoming and outgoing encryption for these: IP Addresses

This setting can be used to force the IP addresses you specify to use your configured settings for inbound and/or outbound transmission.

- You MUST NOT force encryption on the IP address between the Email Protection server and your Web server.

Encrypt Message Content

If you use a non-PGP® server to encrypt message content and wish to use Email Protection to filter outbound messages, contact our support team at support@norman.com. They will help you create a custom sieve script for this purpose.

The Console settings are used ONLY if you have the PGP® Email Gateway server.

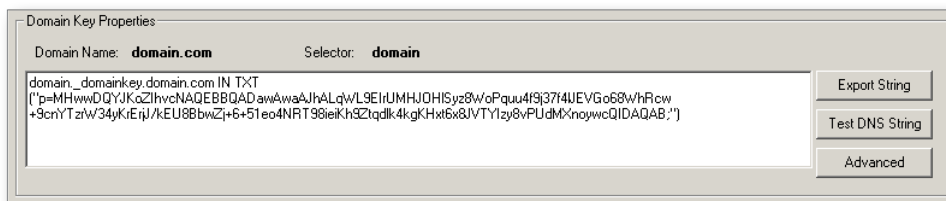
Domain Keys

From this panel, you can configure DKIM (Domain Key Identified Mail) for Email Protection.

Domain Keys is a method of authentication that uses public keys and the DNS to establish the origin and contents of an email message. It allows for near end-to-end integrity from a signing to a verifying Mail Transfer Agent (MTA) and is independent of SMTP routing.

Use the following instructions to configure DKIM signatures on outbound messages:

1. Click **Enable DKIM signing for outbound messages**
2. In **Domain Key Configuration**, click **Add**.
3. Enter your **Domain Name** (e.g. domain.com) where indicated.
4. In the **Selector** box, enter a word of your choice. This will be used as a secondary identifier for the domain.
 - For security reasons, do not use the same word for more than one domain.
 - The **Edit** button can be used to change the selector, but you MUST also replace the DNS string on the DNS server after doing so.
5. When you click **OK**, your public key appears in the **Domain Key Properties** window.



6. The public key string must be copied into your DNS text record. Click **Export string** to copy the string to a text file.

Follow the steps below to configure the DNS record.

Note

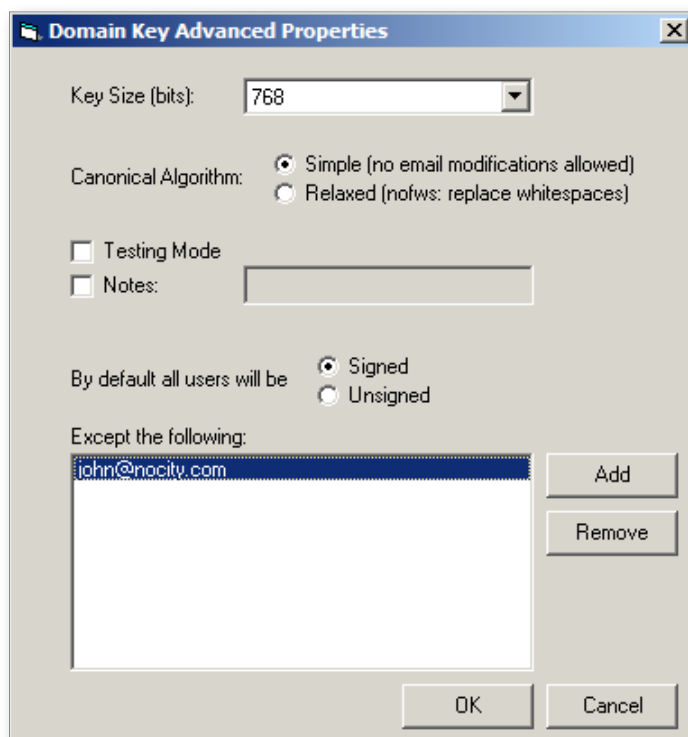
These instructions are specific to Microsoft DNS Server, but should be similar for other DNS servers:

7. Open the DNS Server console and expand **Forward Lookup Zones**.
8. Right-click the domain and select **New Domain**.
9. In **New DNS Domain**, enter `_domainkey` and click **OK**.
10. Right-click `_domainkey` and select **Other New Records**.
11. In **Resource Record Type**, select **Text (TXT) > Create Record**.
12. In **Record Domain**, enter a name for the record (e.g. DKIM).
13. In the **Text** field, paste the public key string copied from the Email Protection Console.
14. If using Microsoft DNS: do NOT copy the parentheses or the quotation marks that are displayed at the beginning and end of the supplied string (e.g. only copy the content between the marks, as below):

```
p=MHwwDQYJKoZIhvcNAQEBBQADAwAwAAJhAO0kPmcqXXdTvieToYfhIA2HdoT/k4P5aoj0bHnZgNrP24jaOZ1TKYE+QsdSTOJE5blqSNie7alGMC+y/VrKW907dMCZyY3Rnwa08dStII9VAfr2Of/Z6i8bW/YAExnvRHQIDAQAB;
```

If using Bind DNS, you MUST use the parentheses and quotation marks, i.e. copy the entire string as supplied.
15. Exit the DNS Server console and return to the DKIM panel in Email Protection.
16. Click **Test DNS String**. If you had created strings for multiple domains, select a domain name first in the **Domain Key Configuration** table before clicking **Test DNS String**.
17. If the test is successful, click **Enable** to activate the signature.
18. To delete a signature, select the domain name and click **Remove**. You must also remove the DNS string from the DNS server.

Advanced settings



You can optionally use this panel to modify the key structure:

Any changes made to the following properties will change the DNS string. Therefore, you must also replace the string text on the DNS server.

Key Size: use this to optimize performance (default is 768 bits).

- Larger numbers will reduce performance but will increase the difficulty of breaking the signature.

Canonical algorithm: used to determine how the header is handled:

- **Simple** (default): tolerates almost no modification of the email message in transit.
- **Relaxed:** tolerates common modifications such as whitespace replacement and header field line rewrapping.

Testing Mode: use this feature to signal to the receiving server that you are testing the signature. The receiving server treats unsigned messages with the same importance as signed messages.

- Receiving servers must not treat messages from signatures in testing mode differently from unsigned email, even should the signature fail to verify.

Notes: you can add comments to the public key string which will not be interpreted by the receiving server (limit of 265 characters).

- This tag should be used sparingly because the DNS server has space limitations.

Signed/unsigned: you can configure Email Protection so that all users are either signed or unsigned.

- You can specify an exception list by clicking **Add**.

How DKIM Works

When a message is sent out through Email Protection, DKIM adds a header (DomainKeys-Signature:) that contains a digital signature of the message contents. The receiving SMTP server uses the name of the sending domain, the `_domainkey` string and a selector from the header to perform a DNS lookup. In turn, the returned data includes the domain's public key. Immediately after the DomainKeys-Signature: header, the receiving email server decrypts the hash value in the header and recalculates the hash value for the message contents. If the two values are a match, it proves, cryptographically, that the email message originated from the intended domain and that the message was not altered in transit. The way in which forged messages are handled is left to the discretion of the receiving server's administrator.

While DKIM does not prevent email abuse, it allows abusive domains to be tracked and detected, thus helping to prevent fraud. By identifying the sender's domain, domain-based trusted and blocked senders lists are more effective, as is detecting phishing. The absence of a DKIM signature indicates that email could be forged (i.e. a forged source email address or domain).

Please consult the following RFC for more information:

<http://www.rfc-editor.org/rfc/rfc4871.txt>.

Content Filters

Overview of content filtering

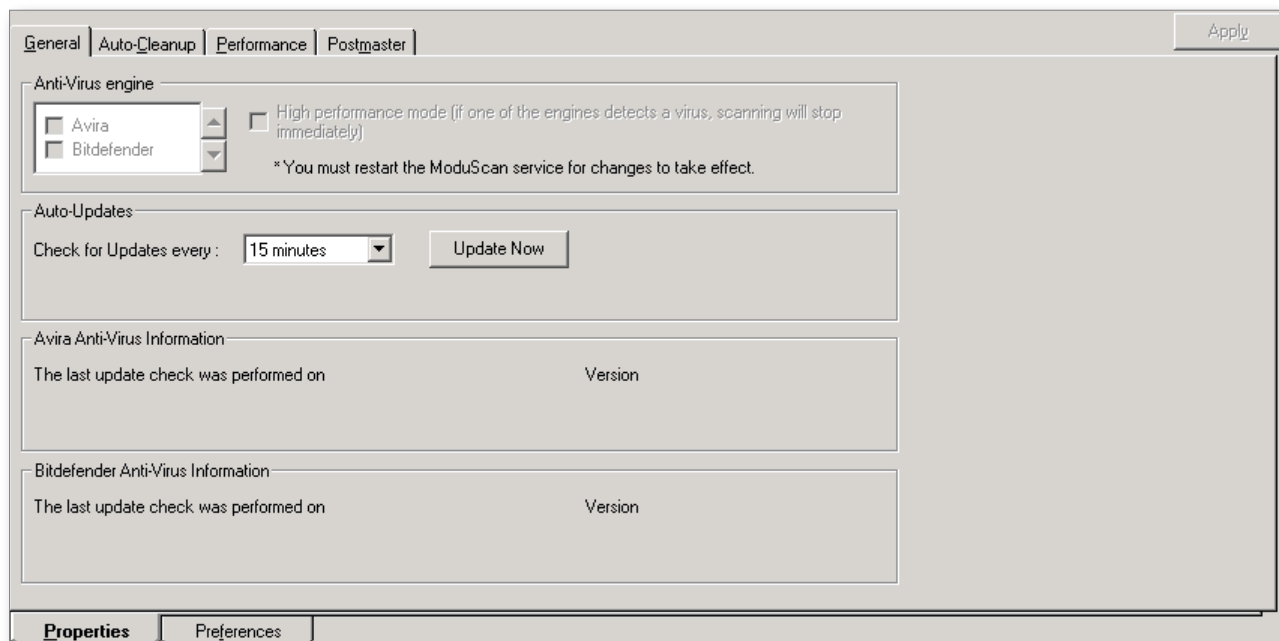
The following sections describe the content filter controls.

- Each filter type allowed by your license (virus, attachment and/or spam) is enabled system-wide when Email Protection is installed, and set to the highest level of security.
- Domain and User settings exist for all filter types to provide greater flexibility and user control over scan aggression levels.
- Filter settings can be customized per domain and/or user in the console. But permission controls exist to optionally allow users to adjust their own settings through the use of WebQuarantine, Quarantine Reports and/or directQuarantine. Any changes users make will be visible in the console.
- Administrators have ultimate control over all filters through the use of master switches at the system level. These switches allow you to turn filters on or off system-wide, to force certain settings for all users, or to set special permissions for select users.

In general, Email Protection checks for and applies the scan controls in this order: 1) User, 2) Domain and 3) Server.

Navigating the filter settings

Where indicated, the filter controls are separated into 2 layers of tabs: **Properties** and **Preferences**, located at the bottom of the main panel. Properties contain system-level controls only; preferences contain the controls that can be customized per domain or per user.



Virus

Virus scanning is automatically enabled to scan inbound messages from the Internet (in the versions that support this feature). If you also wish to scan users' outbound email, you must configure your Exchange (or other email server) to route outgoing messages to Email Protection prior to sending to the Internet.

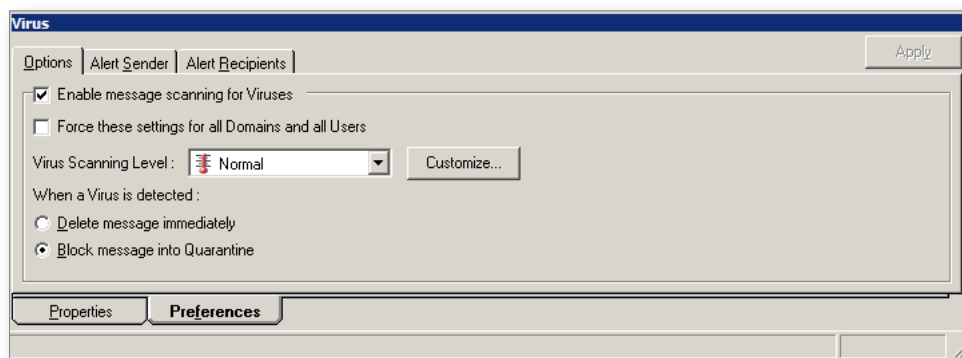
Messages are always scanned for dangerous content prior to spam scanning. For better performance, attachments are filtered first, before viruses, however this order can be changed in the **System > Scanning Order** settings (see "Scanning order" on page 27).

Preference settings

The default view is of the Properties tab. However this section begins with the Preference settings, which is where you set the scan levels and message handling rules. These are the settings that can be customized at the Domain and User levels.

Options

Enable message scanning for Viruses is enabled by default. If you wish to disable virus scanning for the entire system, turn this feature off.



Force scanning for all Domains and all Users

- Overrides individual settings for users and domains and forces a virus scan on all messages.
- Do not use this function if you plan to allow domains and users override privileges.

Virus Scanning Level

- Used to select the scanning level: Normal, Customized or Disabled.
 - **Normal**: the default setting, this will block infected files in addition to those that are considered corrupt or cannot be scanned for any reason.
 - **Customized**: can be used to deselect corrupt/unscannable files if there are any issues with false positives. Click on the **Customized** button to select the desired options.
 - **Disabled**: if selected, virus scanning is turned off.

When a virus is detected:

Choose one of the following options when a virus is found:

- Delete message immediately
- Block message into Quarantine

Alert Sender

This feature enables you to specify if and how to notify the sender that the message contained a virus.

Due to current behavior of spam and malware that spoof sender addresses, do NOT use this option. If enabled, false notifications are likely to be sent to people who did not actually send the virus.

Alert Recipients

This feature allows you to specify if and how to notify the recipients when a message contains a virus.

Both directQuarantine and/or Quarantine Reports clearly label the messages that contain viruses, so you may want to use those features instead of the notification process.

Enable Alert Notifications to Recipients

- This must be turned on at the server level to be able to set individual controls at either the domain or user levels.

Recipients receive notification

- This server-level override function allows you to reset individual domains and/or users' settings to force everyone to receive alerts.
- Enter the Name, Address and Subject for the alert messages.

Select the message to be used for the alert:

- Use the default message.
- Use message from file: create a custom TXT or HTML file containing the notification text, and browse to select the file name.
- Use current message (plain text): enter your text in the window below.

Attach cleaned message

- When enabled, a copy of the cleaned message (without the virus) will be sent as an attachment to the notification email.
- If the virus cannot be removed, the message will be quarantined.
- When disabled, the recipient will only receive notification of the email message while the original is quarantined.

Encoding

- Specify the text format: either Text / plain, or Text / HTML.
- Remember to enter the HTML code in the message body or specify an HTML file if you are pointing to a file.

Alert Substitutions

In the alert notifications, you may use two substitutions that will insert text based on the message being scanned and the results of the scan:

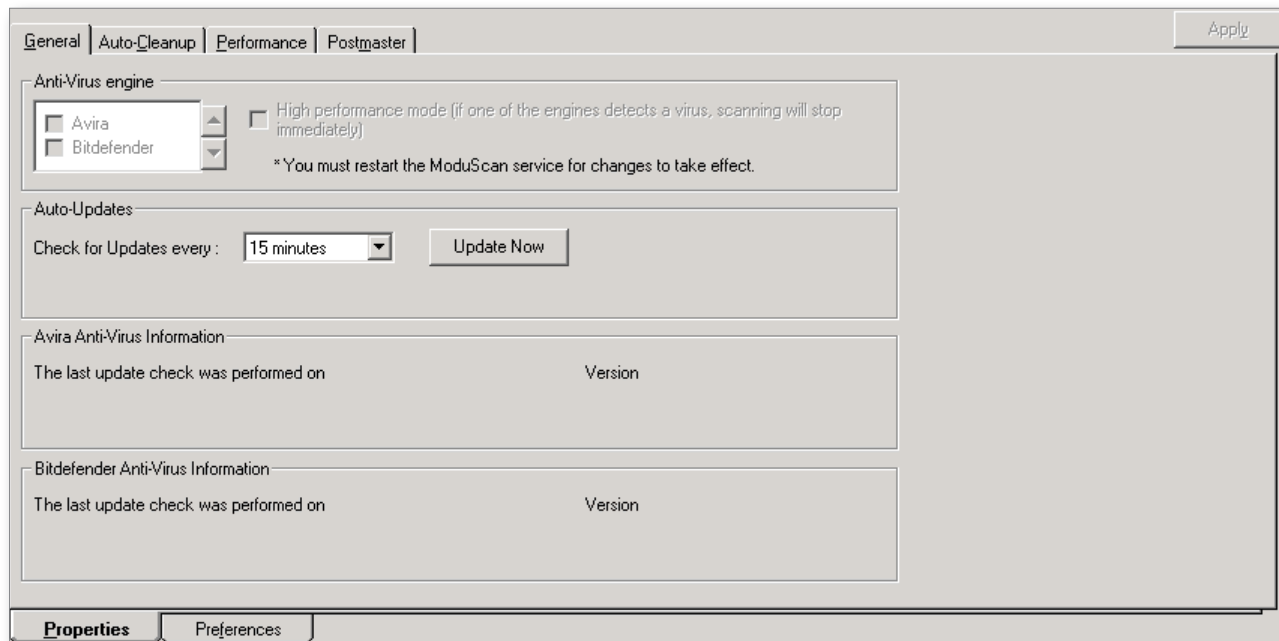
- Insert the sender name of the infected message: enter %1!s!
- Insert the scan report from the anti-virus engine: enter %2!s!

Properties settings

The following sections describe the settings in the Properties tab (the default view of the Virus panel). These settings exist at the system-level only.

General

This panel provides general information about the virus scan engine and the update process, including the last online update check and when the last download of the virus definitions occurred.



The information you see in this panel will depend on your licensed version, and may display update details for the Avira engine, the Bitdefender engine, or both.

View last update info

- This opens a text file which provides the URL for new virus signature information on the Avira/Bitdefender website.

Accept automatic high priority virus definition updates

- Virus definition updates are tested for quality. However, there may be emergency situations when the definition files are made available prior to quality assurance tests.
- If you choose to receive these signature files without waiting for quality assurance testing, check this option and they will be sent to you as soon as they are available.

It is recommended that you leave this feature disabled unless you require a time-critical update. As the files have not passed quality assurance testing, we cannot guarantee that these files will run properly, which may cause system problems.

Check For Updates Every

- Use the drop-down menu to select when your Email Protection server checks for virus definition files.
- The system is automatically configured to check for new definitions every 15 minutes.

Update Now can optionally be used to force an immediate update of the files.

Auto-Cleanup

These settings allow you to specify when a message is deleted from the virus quarantine.

Messages are removed from both the quarantine folder and the database when the expiry date is reached, or when the maximum total size is reached - whichever comes first.

You may optionally modify these settings:

- **Message expires after:** enter the number of days.
- **Max. Total Size:** enter the number of KB.
- **Start job at:** enter a time using the format hh:mm.

Performance

These settings enable you to set parameters to improve the performance of the anti-virus engine.

Enable Performance Caching

- Performance caching enables Email Protection to recognize messages that have previously been scanned for viruses. When a message with the same virus enters the email system, it is treated like the original.
- Virus scanning does not occur for these messages: they are immediately quarantined or deleted according to your settings.
- This feature is useful when dealing with Internet worms that can send hundreds and thousands of copies to a email server at one time.
- The infected file is only scanned once but all copies are treated in the same manner as the first one.

Cache Size: Specify the number of entries to be kept in the performance cache.

Keep in Cache for: Specify the lifetime of a cache entry. Once time has expired, the entry will be removed from the cache.

Enable Attachment's size verification

- You can restrict scanning for large attachments (which can potentially slow system performance).
- Enter the maximum file size in KB.

Postmaster

You can optionally specify a Postmaster mailbox to receive notifications when a virus is detected.

- **Send Notifications to Postmaster:** Enable to enter a postmaster mailbox. This must be a valid address on your email server.

Domain virus controls

Virus settings can be configured at the Domain level in the Console:

Go to **Domains > select domain name > Virus**

Enable **Override server default settings**:

- Override cannot be selected if **Force scanning for all Domains and all Users** is checked in the system settings under **Virus > Preferences > Options**.

- Configure your preferences for scanning level, message handling and recipient notifications.
- Do NOT enable **Senders Receive Notification** (see “Alert Sender” on page 54).

User virus controls

Virus settings can be configured at the User level in the Console:

Go to **Users > select user name > Virus**

Enable **Override domain default settings**:

- Override cannot be selected if **Force scanning for all Domains and all Users** is checked in the system settings under **Virus > Preferences > Options**.
- Configure your preferences for scanning level, message handling and recipient notifications.
- Do NOT enable **Senders Receive Notification** (see “Alert Sender” on page 54).

Phishing

Overview

Phishing spam has become more prevalent and, as such, Email Protection isolates it as a separate feature. Messages with phishing content are handled like viruses. However, the scan behavior actually mimics that of spam: the definition files are updated by the spam engine and, by default, the update occurs every 15 minutes. Because of this design, only a Preferences panel exists containing the scan Options (detailed below).

Options

Force scanning for all Domains and All users

- Overrides individual settings for users and domains and forces scanning on all messages.
- Do not use this function if you plan to allow domains and users override privileges.

Scanning Level

- Select the level of aggressiveness for scanning from Disabled, Normal, Strong or Extreme:
 - **Extreme**: With this option, everything categorized as Extreme, Strong and Normal will be blocked.
 - **Strong**: Only messages categorized as Strong and Normal are blocked.
 - **Normal**: only the Normal group is blocked.
- Extreme is set by default, but may produce False Positives. If this occurs, reducing it to Strong should provide a good balance between protection and little-to-no false positives.

When Phishing is detected

Choose one of the following options for message handling:

- Delete message immediately
- Block message into Quarantine

Allow users to release phishing messages

- This enables users to release phishing messages from quarantine in the event of a false positive.
- This feature can be enabled for specific users only, if desired. See the information below.

Domain phishing controls

Phishing settings can be configured at the Domain level in the Console.

Go to **Domains > select domain name > Phishing**

Enable **Override server default settings**:

- Override cannot be selected if **Force scanning for all Domains and all Users** is checked in the system settings under **Phishing**.
- Configure your preferences for scanning level, message handling and whether members of this domain can release phishing messages from Quarantine.

User phishing controls

Phishing settings can be configured at the User level in the Console.

Go to **Users > select user name > Phishing**

Enable **Override domain default settings**:

- Override cannot be selected if **Force scanning for all Domains and all Users** is checked in the system settings under **Phishing**.
- Configure your preferences for scanning level, message handling and whether this user can release phishing messages from Quarantine.

Spam

Spam scanning is automatically enabled to scan inbound messages from the Internet (in the versions that support this feature). If you also wish to scan users' outbound email, you must configure your Exchange (or other email server) to route these messages to Email Protection prior to sending to the Internet.

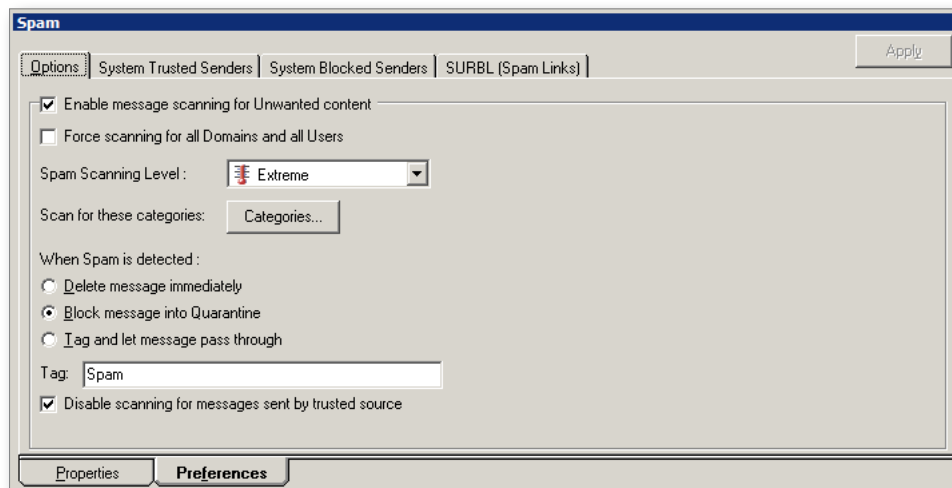
The spam controls are separated into 2 layers of tabs, **Properties** and **Preferences**, located at the bottom of the main panel.

Preference settings

Beginning with the Preference settings, this is where you set the scan levels and message handling rules. These settings can be customized at the Domain and User levels.

Options

Use these settings to configure spam scanning for the entire system.



Force scanning for all Domains and All users

- Overrides individual settings for users and domains and forces scanning on all messages.
- Do not use this function if you plan to allow domains and users override privileges.

Spam Scanning Level

- Select the level of aggressiveness for scanning: Disabled, Normal, Strong or Extreme.
 - **Extreme**: With this option, everything categorized as Extreme, Strong and Normal will be blocked.
 - **Strong**: Only messages categorized as Strong and Normal are blocked.
 - **Normal**: only the Normal group is blocked.
- Extreme is set by default, but may produce False Positives. If this occurs, reducing it to Strong should provide a good balance between protection and little-to-no false positives.

Scan for these Categories

The spam filter categorizes messages based on their content. Click **Categories** to view the message types. Select which ones you want scanned, and uncheck those that should bypass the scan and be delivered.

When spam is detected

Select one of the following message handling options:

- Delete message immediately.
- Block message into quarantine.
- Tag and let message pass through:
 - Enter a tag or label to be added to the Subject line of a message (e.g. Spam).
 - This option is useful for those who prefer to receive all messages, but have their own filtering or rules mechanisms enabled in the email client. The email rules can then determine what to do with messages based on the subject tag.

Disable scanning for messages sent by trusted source

- This function is used specifically for users who authenticate using SMTP Auth, to allow their outgoing email to the Internet to bypass spam filtering (including the filter and custom scripts.)
- Incoming Internet email will be scanned according to your settings.
- Attachment and virus scanning in the Email Protection versions that support these functions will continue.

System Trusted Senders

Trusted senders are the people who are well known to you and whose email content you trust. These settings enable you to specify these known senders, allowing their email to bypass spam scanning and be delivered. Messages from trusted senders will continue to be scanned for viruses and forbidden attachments, however.

This feature is disabled by default.

Enable Auto-Trusted List

Trusted Sender settings exist at the system, domain and user levels. These lists must be manually created and updated, which can be tedious and difficult to maintain.

The Auto-Trusted List instead provides an automated method for creating and maintaining the addresses, based on users' email behavior:

- When a person replies to an email that was originally sent from a local user (who has an account on your Email Protection server), the responding address is automatically added to that user's Trusted Senders List.
- Auto-trusted addresses are not added to the System list.

EXAMPLE

john@yourcompany.com sends a message to anna@gmail.com. By replying to John's original message (i.e. she does not create a new message), anna@gmail.com is automatically added to John's auto-trusted list.

To support the auto-trusted feature, the Default database configured for use with Email Protection must be a SQL or SQL Express Server. (Access and PostgreSQL are not supported).

- To verify the Default database, go to **System > System Databases > Default Database Settings**.

Enable automatic cleanup of old records

This option applies only if the Auto-trusted feature is enabled.

- It automatically maintains the auto-trusted list to keep only the active addresses.
- Cleanup occurs once daily when a user's maximum limit has been reached.
- Addresses in the auto-trusted list are time-stamped upon reply and the automatic cleanup feature deletes the data with oldest time stamps.

- Reoccurring addresses are time-stamped as they enter the database.
- There is a second automatic cleanup process whereby Email Protection looks for mailboxes that have been deleted and removes all auto-trusted entries associated with them. This process occurs every 90 days and is not configured in the Console.

Maximum number of auto-trusted addresses allowed per user

- Enter the maximum number of addresses permitted per user. The default is 1,000.

Additional information about the Auto-Trusted List

- It can only be configured at the system level.
- Is disabled by default.
- Auto-trusted addresses are added to each user's trusted senders list but are not visible to the users.
- Because auto-trusted entries cannot be viewed or edited, blocked senders lists take priority during scanning.
- An X-SCA-Stop header (X-SCA-Stop: [autotrust]) appears when a message is auto-trusted and is used by moduscan to display the sieve script execution results.
- When the maximum number of addresses is reached, the record with the oldest timestamp is removed.
- The email server's IP address must be listed in the routing table in Email Protection Console (see [Connections](#)).
- When recipients reply to messages sent from local users, the originating IP address will be compared to the routing table to establish 'trusted' local users and build their auto-trusted lists.

Enable System Trusted Senders List

Create a list of trusted domain names and email addresses that will bypass the custom Blocked Senders List, the filter engine and your custom sieve scripts. This is especially useful if you experience false-positives.

- Addresses in this list apply system-wide.

Click **Add** to enter addresses:

- Domain names and email addresses are supported.
- Wildcards are supported (e.g. *@domain.com).

System Blocked Senders

Blocked Senders are the addresses from which you never want to receive email.

Enable Blocked Senders List

Click **Enable** to create a list of domains and email addresses that will always be blocked, regardless of the content.

Click **Add** to enter addresses:

- Domain names and email addresses are supported.
- Wildcards are supported (e.g. *@domain.com).
- It is possible to block an entire domain, but allow email from a specific address in that same domain.

EXAMPLE

Block all addresses from xyz.com by entering *@xyz.com to the Block List. Then add john@xyz.com to the Trusted Senders List. All email from the xyz.com domain will be blocked except John's.

When a message is received from a Blocked Sender

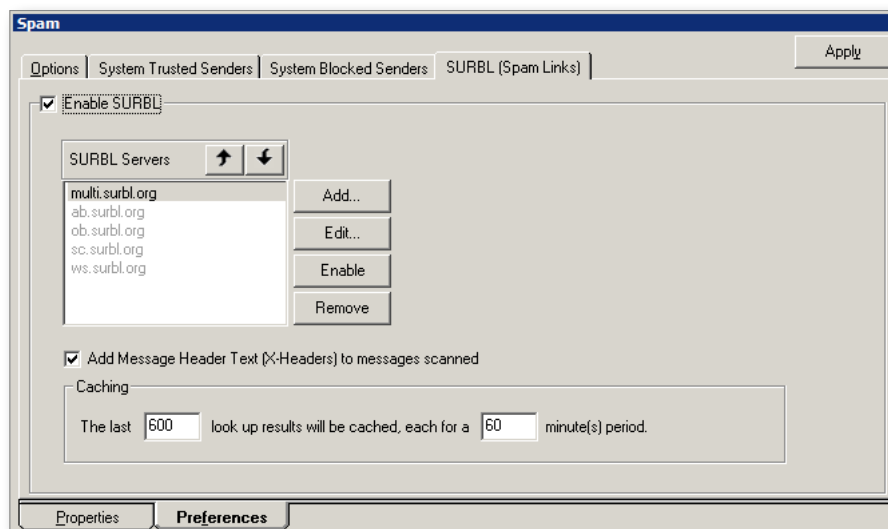
Select one of the following message handling options:

- Delete the message
- Send to quarantine
- Send to recipient with tag: Enter text to be added to subject line and the message will be delivered instead of blocked.

SURBL (Spam Links)

SURBLs differ from most other RBLs in that they are used to detect spam based on message body URLs (these are links - usually websites). Unlike most other RBLs, SURBLs are not used to identify spam senders. Instead, they allow you to identify messages that have spam hosts mentioned in the message bodies.

The lookup of email URLs is performed randomly, in case spammers bracket spam links in the list with legitimate links at either end of the list.



To use this feature:

- Click **Enable SURBL**.
- Select a server from the list provided.
- Click **Enable > Apply**.

You may optionally **Add**, **Remove** and **Edit** SURBL servers, and use the Up and Down arrow keys to move a server name in the list to alter priority. The list is applied in order from top downwards.

Add Message Header Text (X-Headers) to messages scanned

X-Headers can be added when a message matches a DNS blacklist entry and when it fails a validation test.

- These headers are used by the spam scanner.
- This function is enabled by default.

Caching

Configure how many lookup results will be cached and for how long.

Properties settings

General

This panel provides update and version information for proprietary spam filter, called Sequential Content Analyzer (SCA).

- The spam definitions used by the SCA engine are updated automatically and cannot be customized.

Auto-Updates

The spam engine and its definition files are updated automatically by Email Protection. It is set to look for new definitions every 15 minutes, which are applied automatically as they become available.

- You may optionally change this frequency.
- These updates only affect the filters that we supply. Any custom scripts you create will remain intact.

Auto-Cleanup

These settings allow you to specify when a message is deleted from the spam quarantine.

Messages are removed from both the quarantine folder and the database when the expiry date is reached, or when the maximum total size is reached - whichever comes first.

You may optionally modify these settings:

- **Message expires after:** enter the number of days.
- **Max. Total Size:** enter the number of KB.
- **Start job at:** enter a time using the format hh:mm.

Domain spam controls

Most spam scan preferences can be configured in the Domain properties in the console but there are some exceptions:

- Enabling **Force scanning for all Domains and all Users** in the System-level Spam settings will block the use of Domain overrides.
- Auto-trust sender settings are available at the System level only.
- SURBL settings are available at the System level only.

To configure Domain overrides:

Go to **Domains > select domain name**, and select the **Spam, Trusted Senders**, and/or **Blocked Senders** tabs. Enable **Override server default settings** and configure your preferences.

User spam controls

To configure User overrides for spam settings:

Go to **Users > select user name > Spam**.

- Enable **Override domain default settings** and configure your preferences.
- Enabling **Force scanning for all Domains and all Users** in the System-level Spam settings will block the use of User overrides.

Trusted Senders and **Blocked Senders** also have user-level settings. Any addressees that users enter manually will be visible in these screens.

- If you had enabled the Auto-trust feature, those addresses will not be visible here. See “System Trusted Senders” on page 61 for details.

Forbidden Attachments (F.A.)

You can block attachments by name or type which can help to prevent new types of viruses and unwanted content from entering your system.

The Forbidden Attachment controls are separated into 2 layers of tabs: **Properties** and **Preferences** (seen at the bottom of the panel). This section begins with the Properties settings, which is where you can configure the list of attachments to filter.

General

From this panel, you can set general properties for the attachment scanner.

Enable Smart File Type Detection (Fingerprinting)

- Used to enable Fingerprinting, a method by which the real attachment type of a specific file is detected.
- This blocks questionable attachments that have been renamed.

EXAMPLE

update.doc has been renamed to update.txt. Fingerprinting will be able to detect that the file is actually a Word document.

Block zip files encrypted with a password

- Enabling this features ensures all zip files that have been password-protected are blocked from entering your email system.

Automatically quarantine messages with attachments larger than

- When enabled, all messages with attachments larger than the specified size (in KB) will be quarantined.
- A value of "0" means that there is no limit.

Forbidden Attachments

This screen provides a ready-made list of attachments that will automatically be blocked by Email Protection, such as *.BAT, *.EXE and other files that often carry viruses and other malware. However, as an administrator, you can completely customize the contents of this list for the system as a whole (i.e. the attachment list cannot be adjusted at the domain or user levels).

The files are grouped by severity (Normal, Strong and Extreme) to correspond to the filter aggression levels. Expand the groups to see the file names.

As with all other filters, the scan aggressiveness level for forbidden attachments can be adjusted at the system, domain and user levels. However, the list of file attachments can only be configured in this system-level panel.

How to customize the list

Use **Add** to enter a new attachment type and to select the filter level.

- Wildcards are accepted in the names.

Import will import a list from a text file.

- Using Import will overwrite the current list.
- This file must contain text strings with wildcards, separated by a return.

Export will export the list to a text file.

Default will revert the entire list back to default content and levels.

Using the **Edit** button provides a number of options:

It can be used to change an existing file name and/or filter level, including the items in the supplied list.

EXAMPLE

*.DLL files are under the Strong category, but can be moved to Normal by using Edit.

Being able to move files is especially useful if you want to set different scan levels for different people.

Scenario: you want to allow specific file types through for some users (Group A), but to block those files for all other users (Group B). Before making any changes, you need to know how the scan levels work:

- **Extreme**: ALL message types are blocked, including Extreme, Strong and Normal.
- **Strong**: messages in both the Strong and Normal groups are blocked.
- **Normal**: only the Normal group is blocked.

Returning to the scenario: to block file types for the majority of users (in Group B), place the files in either the Strong or Extreme category, and set the equivalent scan level for the Group B users. Because the users in Group A must receive those files, set their scan level lower: to Normal.

Auto-Cleanup

These settings allow you to specify when forbidden attachments are deleted from the quarantine.

Messages are removed from both the quarantine folder and the database when the expiry date is reached, or when the maximum total size is reached - whichever comes first.

You may optionally modify these settings:

- **Messages expire after**: enter the number of days.
- **Max. Total Size**: enter the number of KB.

Postmaster

You can optionally notify the system Postmaster when a forbidden attachment is detected:

- Enter the name of the postmaster (default is Postmaster).
- Enter the email address for the postmaster account. This must be a valid account on the system.

Preference settings

Use the bottom tabs to access the Preference settings to configure the system-level scan controls.

Options

Set the scan level and message handling rules for the attachment-blocking engine.

Detect forbidden attachments within compressed files

- Scans compressed files for forbidden attachments.

Force scanning these Settings for all Domains and all Users

- Overrides the individual settings for users and domains and forces all users' email to be scanned at the selected level.

Attachment Scanning Level

- Used to select the level of aggressiveness for attachment-scanning: Normal, Strong or Extreme.
- If **Disabled** is selected, attachment scanning is turned off.

Set the message handling options:

- Delete message immediately.
- Block message into Quarantine.
- Allow users to release quarantined attachments: use this option if there are issues with false positives, or if you want to allow users to release certain message types. Note that this option can also be set at the domain and user levels, to provide more control.

Alert Sender

This feature enables you to specify if and how to notify the sender that the message contained a forbidden attachment.

Due to current behavior of spam and malware that spoof sender addresses, do NOT use this option. If enabled, false notifications are likely to be sent to people who did not actually send the attachment.

Alert Recipients

This feature allows you to specify if and how to notify the recipients when a message contains a blocked attachment.

Both directQuarantine and/or Quarantine Reports clearly label the messages that contain attachments, so you may want to use those features instead of the notification process.

Enable Alert Notifications to Recipients

- This must be turned on at the server level to be able to set individual controls at either the domain or user levels.

Recipients receive notification

- This server-level override function allows you to reset individual domains and/or users' settings to force everyone to receive alerts.
- Enter the Name, Address and Subject for the alert messages.

Select the message to be used for the alert:

- Use the default message.
- Use message from file: create a custom TXT or HTML file containing the notification text, and browse to select the file name.
- Use current message (plain text): enter your text in the window below.

Encoding

- Specify the text format: either Text / plain, or Text / HTML.
- Remember to enter the HTML code in the message body or specify an HTML file if you are pointing to a file.

Alert Substitutions

In the alert notifications, you may use two substitutions that will insert text based on the message being scanned and the results of the scan:

- Insert the sender name of the infected message: enter %1s!
- Insert the scan report from the anti-virus engine: enter %2s!

Domain attachment controls

Forbidden Attachment settings can be configured at the Domain level in the Console.

Go to **Domains > select domain name > Attachments**.

Enable **Override server default settings**:

- Override cannot be selected if **Force scanning for all Domains and all Users** is checked in the system settings under **FA**.
- Configure your preferences for scanning level, message handling and whether members of this domain can release attachments from Quarantine.
- The attachment list cannot be customized here.

User attachment controls

Forbidden Attachment settings can be configured at the User level in the Console.

Go to **Users > select user name > Attachments**.

Enable **Override domain default settings**:

- Override cannot be selected if **Force scanning for all Domains and all Users** is checked in the system settings under **FA**.
- Configure your preferences for scanning level, message handling and whether this user can release attachments from Quarantine.
- The attachment list cannot be customized here.

Language Filter

The language filter can be set to block spam based on foreign languages and character sets.

This feature enables you to select which languages to block from a pre-set list. By default, all languages are allowed.

Message handling options include:

- Delete message immediately.
- Block message into Quarantine.
- Tag the message subject and allow it to pass through.

Select language content to block

- Click on » to add a language to the Blocked Languages list
- Click on « to remove language from the Blocked Languages list

Foreign Language Behavior

- Scanning for language content occurs:
 - After virus and attachment scanning
 - After the trusted and blocked lists
 - Before spam scanning by the SCA engine.

- Custom filters based on language content are supported.
- Trusted addresses will bypass language filtering.
- Messages containing words or characters in several languages are given a language probability rating based on the weight of the content.
 - If the bulk of a message is in Italian, it will be considered 'Italian' and this is the code that will appear in the header envelope.
- The probability rating determines whether the message is filtered or not.
- If the bulk of the message is in a 'permitted' language but contains words or characters in blocked languages, the message will pass through.
- Messages considered spam are displayed in the 'high spam probability' section of the Quarantine Reports and can be released by the user.
- The header tag is accessible to sieve scripts and allows for the creation of custom rules based on language, such as exclusion rules.

The accuracy of language filtering depends upon the amount of text in the message body. A higher number of characters ensures better accuracy. Fewer than 256 characters in the message body could result in poor accuracy. This may occur if you have added **Unrecognizable** to the Blocked Languages list.

Performance

From this panel, you can set performance parameters to improve the performance of the spam engine.

Cache Size:

- Used to specify the number of entries to be kept in the performance cache.
- Presently, these options cannot be modified.

Reload Every:

- Used to specify how often Email Protection verifies if there is a new script available and loads it into memory.
- Presently, these options cannot be modified.

Enable Attachment Size Verification

- Used to restrict scanning for large attachments (which can potentially slow system performance).

Do not scan messages with attachments larger than

- By default, the system will not scan messages if they contain attachments that are larger than 950KB.

Domain language filter controls

Foreign language filters can be configured at the Domain level in the Console.

Go to **Domains > select domain name > Language Filter**.

Enable **Override server default settings**:

- Configure your preferences for message handling (delete, block, or tag and pass) and select the languages to filter.

User language filter controls

Foreign language filters can be configured at the User level in the Console.

Go to **Users > select user name > Language Filter**.

Enable **Override domain default settings**:

- Configure your preferences for message handling (delete, block, or tag and pass) and select the languages to filter.

Quarantine management

Overview of features

Email Protection offers several methods for monitoring and controlling quarantined messages, for administrators and end-users alike.

1. The Quarantine panel in the Administration Console: gives the Administrator a global view of all users' blocked messages.
2. Quarantine Reports: summary reports that can be sent to users on a scheduled basis. See "Quarantine Reports" on page 29 for configuration details.
3. WebQuarantine: a web application that users can log into to see a) their quarantined messages in real time, and b) view and modify their filter settings, if allowed.
4. directQuarantine for Outlook: licensed separately but included with Email Protection, this program allows users to view and control quarantined messages in real time, using features built into Outlook.

The following sections will describe all these options.

Console administration

The quarantine panel in the Console allows you to monitor and view messages captured by the attachment, spam and anti-virus filter engines. Any addresses blocked by custom blacklists will also be included.

To capture all filtered messages system-wide, **Block Message into Quarantine** must first be enabled in each of the filter control panels: Virus, Spam, System Blocked Senders (within the Spam controls), Phishing and FA.

These same settings can also be configured at the Domain and User levels.

The panel is divided into 2 sections: the message **Properties**, and the **Results**.

The **Results** section displays a list of all of the quarantined messages, sorted and displayed separately according to the content:

- **Spam** displays messages blocked by the SCA, your custom sieve scripts and the custom blacklists.
- **Attachments** displays messages blocked by the Forbidden Attachment settings.
- **Viruses** displays the infected files.
- **Phishing** displays messages considered to contain phishing content.

A **Find Result** tab displays the search results for the **Find** command when searching for a particular message. See "Find" on page 83.

Using Quarantine Properties

Select a message in the Results list to view the message details in **Properties**:

- **Message**: Shows the body of the quarantined message in the window, along with the From, To, Cc, Subject, Sent date and any attachments.
- **Headers**: Shows the complete message header details.
- **Raw Source**: Allows you to safely view the contents of a message to determine if it should be released (or not) without risk to your email server.

Using Quarantine Results

Click on the tabs to browse messages in Spam, Attachments, Viruses and Phishing: each line in the Results window represents a blocked message.

Refresh

- Refreshes the list of messages in quarantine.
- When users delete items from their WebQuarantine, there is a slight delay before the value is registered in the Results window.

Release

- Releases messages from quarantine and delivers them to the intended recipient(s).
- Viruses cannot be released, by default, but the option can be enabled by making a change in the registry:
 - Open the Registry Editor
 - Go to: `HKEY_LOCAL_MACHINE\SOFTWARE\Vircom\VOPMail`
 - Create a new **DWORD** named `ScanAllowedVirusesRelease`
 - Assign one of the following values:
 - **0** - (default): No virus can be released from quarantine
 - **1** - Only viruses identified as **Possible virus** can be released
 - **2** - All viruses can be released
 - If any other value is used, 0 will be assumed.

Allowing the virus release affects only the console and administrative actions: end-users are never allowed to release viruses.

Delete: Deletes messages from quarantine.

Mark as unread: Marks read quarantined messages as unread.

False-positive

- Only for use with spam.
- A report is sent to us identifying messages that you consider to be legitimate and improperly quarantined.
- The anti-spam team adjusts the filters to prevent future false-positives.

User administration

Quarantine Reports

The System > Quarantine Reports section described the configuration and scheduling of the reports; this section describes the report functionality.

When enabled, Quarantine Reports are emailed to users on a scheduled basis to provide a summary of their quarantine contents. The Reports can be configured to always show all quarantined messages, or to show only the new messages that have arrived since the last report was issued.

NORMAN Quarantine Report

Created on Tuesday, June 21, 2011 8:00:25 AM for [redacted]
[Customize](#) the report content and schedule

[Delete All Contents](#)

These messages need your attention				
Category	Subject	From	Date	Action
Health	C.O.D payment - HYDROCODONE 7	rebbecageralvn@usit.net	6/20/2011 1:48 PM	Release Block
Miscellaneous	Unleash the Power of Your iPh	dms@businesswatchnetwork.com	6/20/2011 10:21 AM	Release Block

High probability of spam				
Category	Subject	From	Date	Action
Health	C.O.D - Discreet Packing, Eas	hazelnidia@paceworldwide.com	6/21/2011 5:07 AM	Release Block
Goods	don't miss out fHalf Price Sa	leanelementsnow@gmail.com	6/21/2011 4:03 AM	Release Block
Health	Includes Amino Acids, Lose 40	petrinamona@bunqi.com	6/21/2011 3:11 AM	Release Block
Health	Trusted Online Pharmacy - Cia	myrtaantonia@addyourprofile.c	6/21/2011 2:27 AM	Release Block
Miscellaneous	Replica Watches Store welcome	shanitamarisha@ilisa.com	6/21/2011 1:10 AM	Release Block
Goods	Rolex.com F	rolax.com F	6/21/2011 12:46 AM	Release Block
Blocked by Rules	Doctors Give You The Truth, C	rtawannagf@eaton.com	6/20/2011 11:47 PM	Release Block

Potentially harmful content				
Category	Subject	From	Date	Action
Virus	Your Federal Tax transaction	Adele_House@irs.gov	6/21/2011 6:10 AM	N/A Block
Virus	Rejected Federal Tax transfer	Dewitt_Henry@irs.gov	6/20/2011 7:04 AM	N/A Block

[Delete All Contents](#)

Report actions

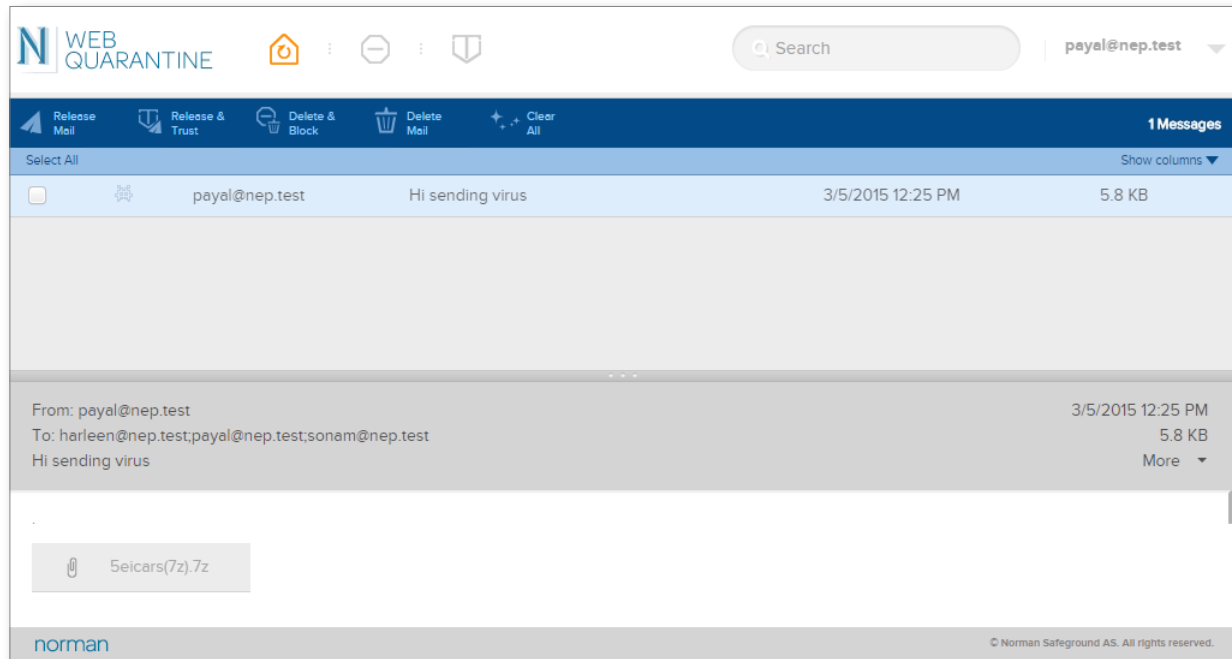
Reports allow users to perform the following functions:

- View the message content by clicking the Subject link: dangerous links within the message are inoperable or blocked.
- Release a message to the Inbox, when permitted (viruses can never be released)
- Additional release options include:
 - The ability to add the sender's email address or domain name to his/her Trusted List
 - Ability to report the message as a false positive: a copy of the message is sent to us so that adjustments can be made to the filters, if necessary.
- Block the message sender: the email address or domain name can be added to the Blocked List
- Delete all messages: deletes only the messages contained in the current report.
- Customize the report content and schedule: if enabled in the console, users can log into WebQuarantine to see their quarantine report content settings and schedule, and make adjustments.

WebQuarantine

This web-based application enables users to log in to see a live, updated view of their quarantined messages and to make adjustments to their settings, including: filter levels, quarantine report contents and schedule, and Trusted and Blocked Sender lists.

All reporting actions available in Quarantine Reports are also available in the WebQuarantine.



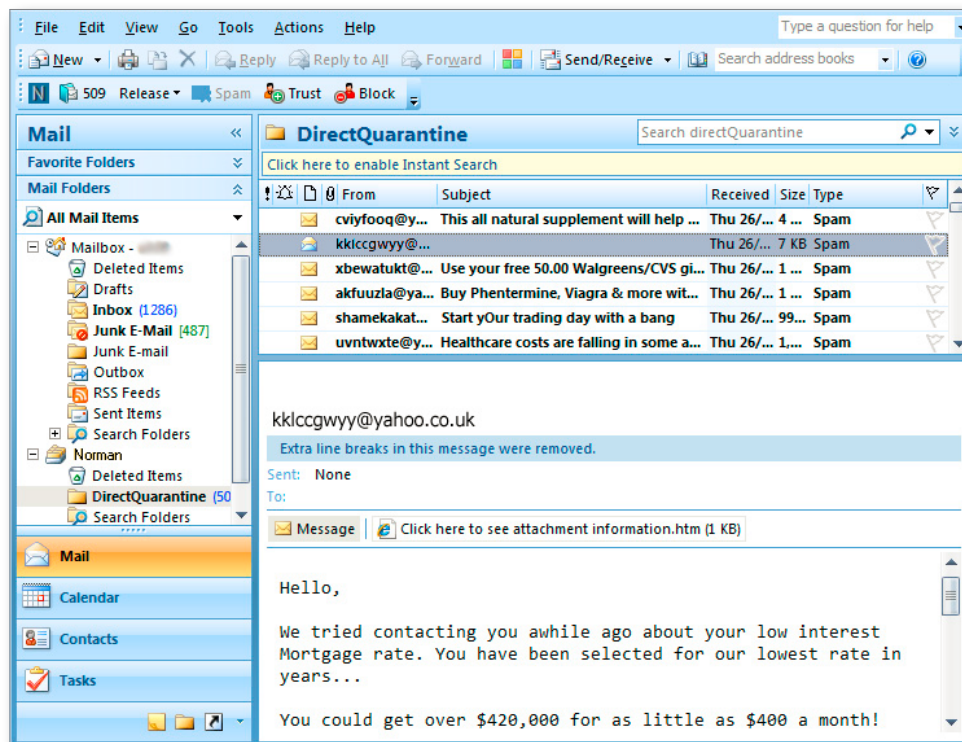
Users cannot change any of the filter settings or other controls without the administrator's permission. Permission controls are located in the Console in **Web > Privileges > Allowed User Properties**. See "Web" on page 81 for details.

A detailed description of this program and its functions can be found in the WebQuarantine User Manual (the document is located on the desktop).

directQuarantine for Outlook

This add-on program to Email Protection provides users with a live, up-to-date view of their quarantined messages directly within Outlook.

Users are able to see the message type (spam, attachment, virus, etc.), and can perform release, delete, block and trust functions, using buttons embedded in Outlook's toolbar/ribbon controls. In addition, users have the ability to report messages as spam, if and when they slip by the filters.



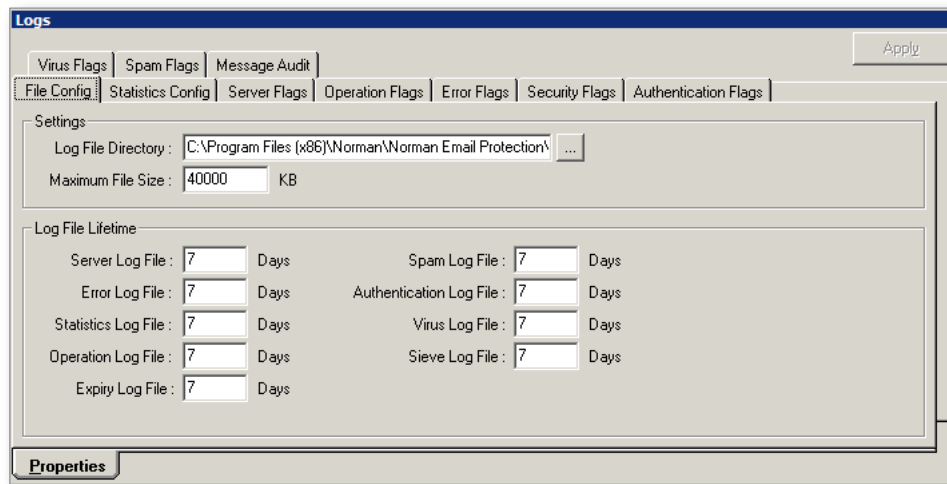
The directQuarantine Server application is installed automatically with Email Protection. It is available for use as a 30-day trial and for licensed users.

The Client application must be installed and configured separately as a Group Policy Object (GPO) on your Active Directory Server. To access the directQuarantine Client installation program and other files, go to **Start > Programs > Norman > Norman Email Protection > directQuarantine Client Install**.

Logs

File Config

This tab contains the core settings for the Email Protection log files: where the files are stored, limits for controlling the log size and for determining how long they are kept.



Logs are text files that can be stored anywhere within your network, including a shared drive. To change the location, enter the full path in **Log File Directory**, click **Apply**, and stop/restart all Email Protection services to register the change in System > Services.

The naming format for the files is **TTTyyyymmdd.LOG**, where:

- **TTT** represents a log type, e.g. OPR (Operation log), ERR (Error log), etc.
- **yyyy** represents the four digits of the year.
- **mm** represents the month, expressed as a number from 1 to 12.
- **dd** represents the day of the month.
- When a log reaches its maximum size, it is renamed with an appended number, e.g. OPRyyyymmdd-1. log, and a new 'active' log begins. The active log is the one without an appended number. The older logs are numbered sequentially.

Maximum File Size: the default size ensures that the log can easily be opened with Notepad or another text editor. If you change the size, simply click **Apply** - there is no need to stop any services.

Log File Lifetime: Enter the number of days a particular log file will be stored on the server.

- At the end of the life span, the files are deleted.
- If the value is set to 0, the files are never deleted.

Below is a summary of the options for each of the log types.

Statistics

Logs the following counters:

SMTPRS

- SMTPRS-NB_CONNECTION
 - Records the total number of connections to the SMTPRS service for all logins
- SMTPRS-NB_RECEIVED_MSG
 - Records the total number of messages received by the service.
- SMTPRS-NB_SERVICE_START
 - Records the total number of times the service has been restarted.

SMTPDS

- SMTPDS-NB_MSG_SENT
 - Records the total number of messages that have been sent by the service.
- SMTPDS-NB_LOCAL_DELIVERY
 - Records the total number of messages that have been delivered to local domains and mailboxes by the service.
- SMTPDS-NB_SERVICE_START
 - Records the total number of times the service has been restarted.

Server

Services Start and Stop: An entry is made whenever a service is started or stopped.

Retry Domain(s): An entry is made whenever SMTPDS is instructed to immediately retry the pending domains.

Change Configuration: This item is not recorded.

The above items can also be logged in the Windows Event Viewer.

Operation

Protocol Exchanges: Logs every SMTP command sent to and response received by the system.

Extended Protocol Exchanges: Logs every extended protocol command sent and response received by the system.

Received Message Data: All message data received by SMTPRS is logged in the operation log file, including the message content.

- This information creates huge log files and should be used for debugging purposes only
- At no time should you enable this feature for every-day use

Transmitted Message Data: All the message data sent by SMTPDS is logged in the operation log file.

- This information creates huge log files and should be used for debugging purposes only
- At no time should you enable this feature for every-day use

Received Transaction Summary: A summary of message receipt is logged. It can also be logged in Windows Event Viewer.

Transmitted Transaction Summary: A summary of the message transmission is logged. It can also be logged in Windows Event Viewer.

Network Connections: Incoming and outgoing network connections are logged.

DNS Transactions: DNS requests sent by Email Protection and the responses received are logged in the operation log file.

- This information creates huge log files and should be used for debugging purposes only.
- At no time should you enable this feature for everyday use.

Dialup Connections: Not applicable to Email Protection.

Scanning Operations: Logs all operations of the scanning engine.

Error

Protocol Command Failures: SMTP failed commands sent and responses received are logged.

Authentication Failures: Failed authentication attempts using SMTP AUTH server are logged.

Network I/O Failures: Failed network I/O operations are logged.

File I/O Failure: Failed file I/O operations are logged.

DNS Failures: Failed DNS operations are logged.

General Errors: Other failure types are logged.

Scanning Errors: All errors involving the MODUSCAN engine are logged.

All items can also be logged in the Windows Event Viewer.

Security

This information ties in with the features found and enabled in the Security panel (see "Security" on page 38)

Reverse DNS: Messages rejected due to a failed DNS Lookup.

RBL: Messages rejected after RBL/DNSBL Lookup.

Anti-Bulk: Messages rejected because of the Block Scan Attack feature.

Relay: Messages rejected because of anti-relaying protection.

MX: Messages rejected for not having a valid associated MX record.

Protocol filter: Messages rejected by the protocol filter.

Reject Address: Messages rejected because the address was blocked.

Reject Host: Messages rejected because the host was banned.

Banned IP: Messages rejected because the originating IP was banned.

SPF: Results of the SPF lookups.

SURBL: Messages rejected because of SURBL lookups.

Authentication

Logs configured from this panel pertain to end-user logins to the web applications.

Valid Login: Logs all valid logins.

Invalid Login: Logs all invalid logins.

Virus

Detected viruses: Logs information about messages containing viruses and the name of the virus.

Spam

Discarded messages: Logs information about messages filtered by the scan engine.

Message Audit

Enable Audit Logging: This is the master on/off control. Unlike the other log types, audit logs can be enabled per domain or per user, but you must first enable this master control to access the log settings in the Domain and User properties.

System-wide: Enables Audit logging for the entire system.

Log expires in: Specify when the log will expire (in days).

Enable Audit Log Auto Shutdown: Temporarily stops auditing in the event of a high load on the server or a database failure.

- When the audit log is shutdown, new messages will not be audited until the load decreases or the database problem is resolved.
- Messages received immediately before the shutdown will be audited but may not be found in the database.

Set Audit Content: Click to select which of the following audit events to log:

- **Select Logging Template:**
 - **Full Logging** logs all results
 - **Basic Logging** logs the most common results
 - **Custom Logging** appears when you manually select the events to log.
- **Select Scan Results to be Logged:** Displays the selected filtering results.
- **Select Status to be Logged:** Displays the selected message processing status. Information is updated dynamically as messages progress through the system and/or are filtered.

This log is processor intensive. To reduce the load on the system, consider doing the following:

- Limit the number of events to log.
- Enable Audit logging for specific domains or users: override settings exist at both the Domain and User levels.

Web

WebAdmin Privileges

This section is subdivided into 2 sets of properties: **WebAdmin** and **Quarantine** (see the lower-level tabs).

Beginning with **WebAdmin**, this panel contains the privileges (or permissions) settings that are used by both the WebAdmin and WebQuarantine applications. These privileges determine what settings users can or cannot change themselves.

Allowed Domain properties: Specify the domain-level settings that an administrator can modify using the WebAdmin console. All options except Message Audit and Domain Keys are enabled by default:

Reporting	Attachment Levels	Blocked Senders
Virus Levels	Attachment Actions	Blocked Senders Actions
Virus Actions	Attachment Alerts	Blocked Senders Max. Size
Virus Alerts	Spam Levels	Message Audit
Phishing Levels	Spam Actions	Domain Keys
Phishing Actions	Trusted Senders	

Allowed User properties: There are two sets of privilege levels for this feature that affect both the WebAdmin and WebQuarantine applications.

- **Administrators** (i.e. System and/or Domain Administrators): These settings determine the user-level properties that administrators can modify using the WebAdmin program.
 - All properties listed below are enabled by default, except Message Audit.
- **Normal Users:** These settings determine what users can modify using the WebQuarantine program.
 - Users do not have access to Message Audit

Reporting Frequency	Phishing Actions	Language Filter Actions
Reporting Content	Attachment Levels	Trusted Senders
Generate Reports	Attachment Actions	Blocked Senders
Virus Levels	Attachment Alerts	Blocked Senders Actions
Virus Actions	Spam Levels	Aliases
Virus Alerts	Spam Actions	Message Audit (Admin list only)
Phishing Levels	Language Filter	

Reset overriding for all Domains: Click to reset all domain-specific overrides to the default system-wide settings. This removes all domain overrides from the Domains panel.

Allowed User types: This feature is available but not required because users are created automatically in Email Protection.

Domain WebAdmin controls

If you have multiple domains, you can set different WebAdmin privileges per domain, as described above.

The **Administrators** section enables you to specify which users will have access to the WebAdmin panel to act as domain administrators.

Click **Add** to select the users who will have administrator rights. These users will be able to modify domain and user settings as defined above.

User WebAdmin controls

From this panel, you can specify which users will have access to the WebAdmin panel to act as domain administrators.

Click **Add** to select the users who will have administrator rights. These users will be able to modify settings for all users as defined above.

Quarantine options

Web users directory: Specifies the directory where users' quarantined messages and custom settings are stored (including changes to filter options, quarantine report contents and schedule settings, and statistics regarding the number and type of filtered messages).

WebAdmin URL: By entering the WebAdmin URL in this field, WebQuarantine and WebAdmin work in conjunction with each other.

EXAMPLE

```
WebAdminURL = http://127.0.0.1/WebAdmin/
```

- The URL must always end with a forward slash '/'
- In WebQuarantine, when users click on Settings, they will be logged on automatically to WebAdmin to configure their mailbox settings.

IP List for Web Servers Authentication: Can be used to specify IPs that have access to the web applications.

- This is not generally used if Email Protection is configured to do internal routing to a single Exchange / email server.

Quarantine advanced

Encoding: Used to specify the default character encoding for WebQuarantine.

- If using Latin characters, keep the default setting, US-ASCII.

Visual settings: Used to specify the number of contacts and messages that appear on each page in WebQuarantine.

- If there are too many contacts or messages to be displayed on one page, page numbers become available, allowing you to scroll through all pages.

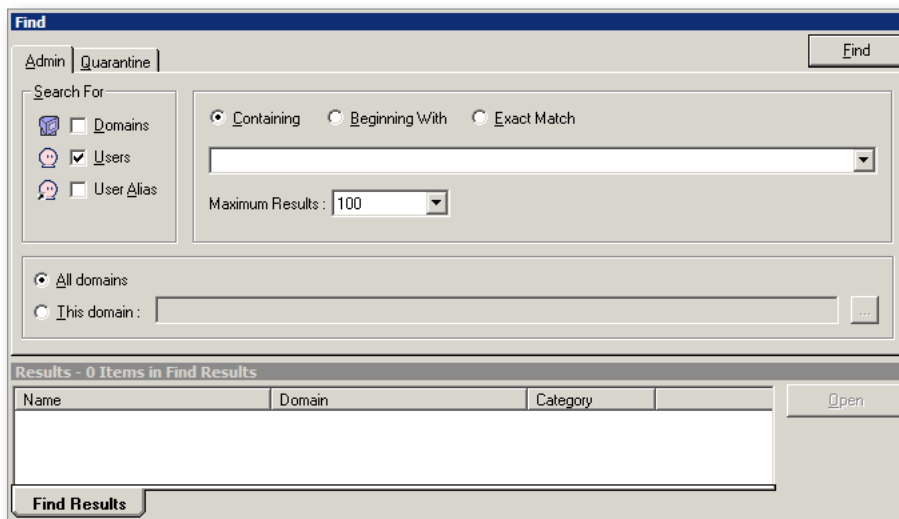
Find

With this feature, you can easily search for users, domains and quarantined messages (where applicable). This feature is convenient if you have multiple domains or a large user base.

Admin

Follow the instructions below to use the Find feature:

1. In **Search For** select **Domains**, **Users**, and/or **User Alias**.



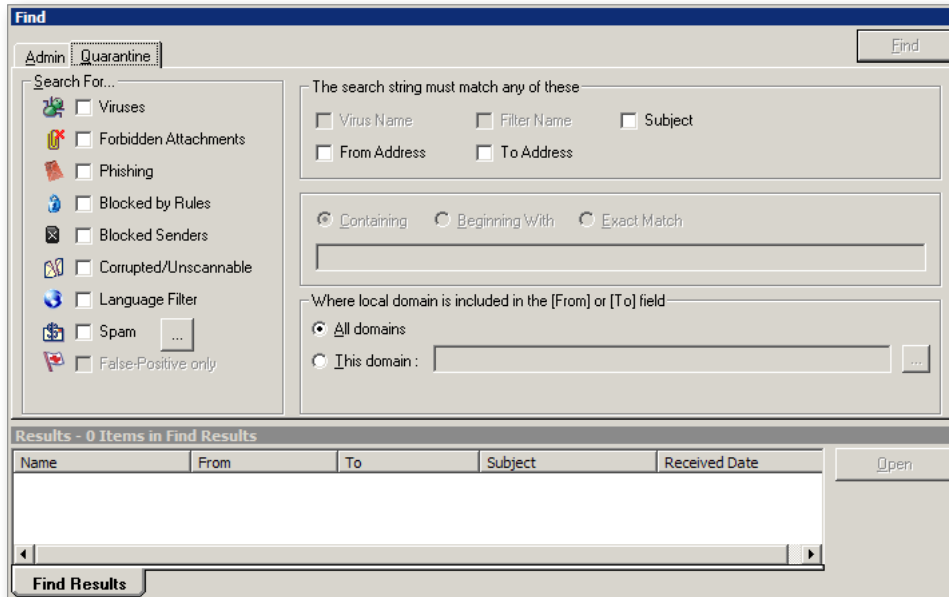
2. Select **Containing**, **Beginning With** or **Exact Match** and enter the text to search.
 - Wildcards (*) can be used.
3. **Maximum Results**: set the number of results to display in the **Find Results** window.
4. Select to search **All Domains** or **This Domain** and enter the name. You can optionally browse the domain list using the ellipsis button (...)
 - The latter function is available if multiple Search For items are checked.
5. Click **Find** to display the results in the Find Results window.
 - Double-clicking an item in the results list will open its properties page.

Quarantine

This feature allows you to search for specific messages in the Quarantine.

1. In **Search For** select one or multiple filter types.

When **Spam** is selected, you can further specify a message category by clicking the ellipsis button (...).



2. Select which **search string(s)** to match.
3. Select **Containing**, **Beginning With** or **Exact Match** and enter the text to search.
 - Wildcards (*) can be used.
4. Select to search **All Domains** or **This Domain** and enter the name. You can optionally browse the domain list using the ellipsis button (...)
5. Click **Find** to display the results in the Find Results window.
 - Double-clicking an item in the results list will open the **Quarantine** panel to display the properties of the selected message.
 - The same Find Results will also be displayed in the **Quarantine > Find Results** tab.

Troubleshooting

Basic Troubleshooting Guidelines

This section provides help for the more common issues you may encounter with Email Protection.

Connection problems with Exchange/AD

Problem:

Email Protection does not seem to be able to connect to Active Directory. Or, when another LDAP Browser is used, a connection still cannot be made.

Resolution:

There may be a network problem such as an improperly configured firewall or network translator. To quickly rule out these problems, telnet from the Email Protection machine to the AD Port (389 or 3268). If something is preventing the connection, the following error will appear:

"Connecting To 192.168.0.112...Could not open a connection to host on port 389: Connect failed"

Problem:

The Exchange Server and Email Protection are not working properly when installed on the same PC.

Resolution:

Open the Exchange System Manager. Go to

Servers > ComputerName > Protocols > SMTP > SMTP Virtual Server. Right-click on **SMTP Virtual Server > Properties**. Make sure the **All unassigned** is selected in the list box and that the port number is changed to something other than Port 25 under the **Advanced** tab.

If you absolutely need to define an IP address, enter the IP address that is specified in Email Protection's **Connection** panel in the Console when you are configuring the connection. Otherwise, the Exchange service will not be reachable.

Problem:

Is my Domain Controller using the Global Catalog?

Resolution:

On your Active Directory Domain Controller, click on

Start > Programs > Administrative Tools > Active Directory Sites and Services

- Expand the site name (by default this will be called "default-first-site-name")
- Expand the Servers folder
- Expand the server to be verified
- Named vs. Default
- Right-click on **NTDS Settings** and select **Properties**
- Check whether the Global Catalog check box is enabled

Problem:

Aliases from other domains are not working or cause unwanted results.

Resolution:

Email Protection supports alias aggregation across multiple domains (i.e. cross-domain alias support). Email Protection considers the primary SMTP address* as the mailbox. The domain specified in the primary address will be the only mailbox listed in Email Protection. All subsequent entries, regardless of the domain, will be specified as aliases in the user's alias list in Email Protection. This keeps mailbox counts accurate and on par with Exchange Server and further consolidates all spam messages into a single quarantine.

If the primary address is specified as an internal Active Directory domain (e.g.: .local), you must either specify your primary SMTP email domain as primary or add an entry for that domain address in the Email Protection **Connections** panel in the Console.

* The SMTP address information can be found in the Active Directory Users and Computers MMC as well as the Recipient policy in the Exchange Service Manager.

Mail delivery problems

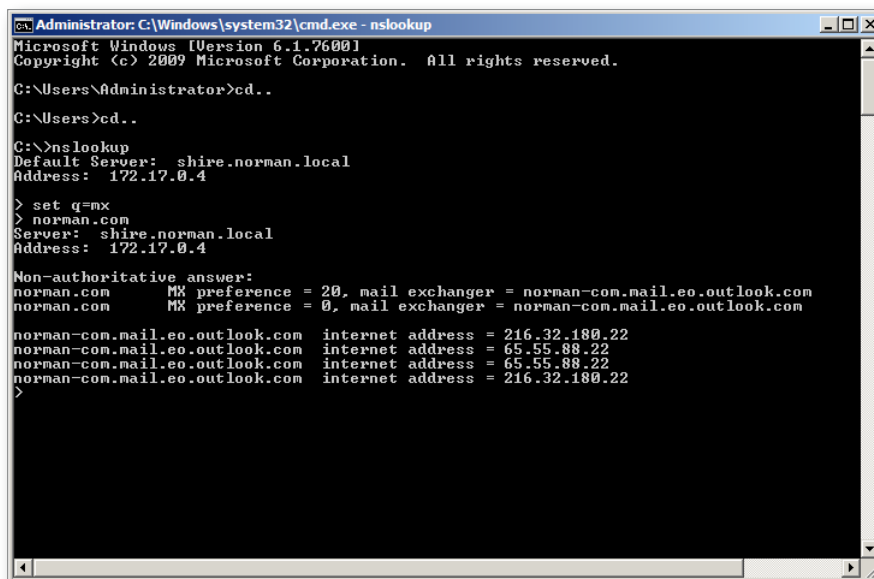
If Email Protection is unable to send outbound email to the Internet, use the following information to try to resolve the problem:

1. To rule out an invalid DNS setting, perform an nslookup of the domain to which users are attempting to send mail:

EXAMPLE

resolve norman.com

- At a command prompt, type: `nslookup <enter>`
- At `>` type: `set q=mx <enter>` to query the MX record
- At `>` type: `norman.com <enter>`



```
Administrator: C:\Windows\system32\cmd.exe - nslookup
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>cd..
C:\Users>cd..
C:\>nslookup
Default Server: shire.norman.local
Address: 172.17.0.4

> set q=mx
> norman.com
Server: shire.norman.local
Address: 172.17.0.4

Non-authoritative answer:
norman.com      MX preference = 20, mail exchanger = norman-com.mail.eo.outlook.com
norman.com      MX preference = 0, mail exchanger = norman-com.mail.eo.outlook.com

norman-com.mail.eo.outlook.com internet address = 216.32.180.22
norman-com.mail.eo.outlook.com internet address = 65.55.88.22
norman-com.mail.eo.outlook.com internet address = 65.55.88.22
norman-com.mail.eo.outlook.com internet address = 216.32.180.22
>
```

The results show that email goes to `norman-com.mail.eo.outlook.com` (pref level 0), and what email address redirection goes to (pref level 20) if this email is down.

2. If the DNS server still has problems when resolving names, perform a lookup using an external DNS server (in this case, Norman's) to verify if your domain can resolve outside DNS servers.
 - At a command prompt, type `nslookup 64.254.224.2 <enter>`
 - If DNS is properly configured, there could be a network connection problem.
 - The email firewall could cause problems:
 - By default, some firewalls, such as Cisco Pix, block the extended SMTP commands required when using SMTP_VRFY or SMTP AUTH connection methods.
3. If the problems appear to be caused by DNS timeouts, two Registry keys can be added to automatically handle the failure. To change the default values, these keys must be created manually. The settings are used by SMTPRS, SMTPDS and MODUSCAN.

To create the registry keys:

1. Click **Start > Run >** enter `regedit` (or Start > and enter `regedit` in the "Search programs and files" box)
2. Go to `HKEY_LOCAL_MACHINE\ Software \ Vircom \ Vopmail`

3. Right-click Vopmail, select **New > DWORD Value**, and enter `DNSFailTimeout`
 - The default value is 30 mins
 - This controls how long to wait (in seconds) before trying the secondary DNS when the primary is down
 - If you wish to change the timeout value, double-click key name, enter the new time in **Value data** and click **OK**.
4. Right-click Vopmail again, select **New > DWORD** value and enter `DNSRetryTimeout`
 - This controls how long (in seconds) to retry the primary DNS server when using the secondary
 - The default value is 1 day

You must restart the SMTPRS, SMTPDS and MODUSCAN services after creating the new key.

Mail pool directories

The message Spool (or queue) contains the message files as they are being processed by Email Protection. The directory is located in `...Norman\Norman Email Protection\Spool`, and contains the following subdirectories:

Invirus

- Contains all messages waiting to be scanned (e.g. virus and spam).
 - Messages found to contain unwanted content are sent to the **Virus** or **Spam** subdirectory, accordingly.
 - Messages containing viruses and spam are then sent to the `Mailboxes\@Quarantine\Inbox` folder (to provide a view of the content to Quarantine Reports, WebQuarantine and directQuarantine).
 - The message headers are written to the quarantine database.
- If none of Email Protection's filters detect suspect content, the message is sent to the **Incoming** directory to begin the delivery process.

Incoming

- This directory receives messages that have first undergone scanning.
- The SMTP Delivery Agent also places messages here, such as non-delivery reports.

Holding

The SMTP Delivery Agent moves messages from the Incoming directory into this directory when attempting to deliver the messages.

Domains

- When a message is moved into the Holding directory, the Delivery Agent creates a subdirectory within the domains directory for each domain to which a message is addressed (e.g. gmail.com, yahoo.com, etc.)
- If the message is for a local user, it creates a subdirectory called `$local$`
- Each subdirectory stores routing information and information about the message recipients on that domain
- The message itself stays in the holding directory until it can be sent to the destination address

Dead

- This directory stores messages addressed to the Postmaster but which cannot be delivered.
- It also collects messages that have caused a email loop.
- A text file describing the reason for their 'death' is provided with the messages.

Diagnosing problems using spool directory contents

After email passes through the security checks, Email Protection processes the messages according to the configured scan settings and follows your quarantine rules.

Resolving an Invirus backlog

In Windows Explorer, go to [...\Norman\Norman Email Protection\Spool\Invirus](#) to verify if there is a backlog of .MSG and RCP files.

Use the Refresh function to verify if the messages are flowing through the Invirus directory in a timely manner.

A backlog with the MODUSCAN engine can be caused by the following:

- Quarantine is slow or corrupt
- There could be a backlog of messages in [...\spool\spam](#) or [...\spool\virus](#)
- Using MS Access for the Quarantine database could cause a problem
 - MS Access has a size limitation of 2GB and, if the database nears 2GB, the MODUSCAN service will spike to 100% CPU
 - Consider using SQL Server or SQL Server Express for the Quarantine database
- If you choose to continue using MS Access, you may need to replace your database
 - Go to [...\Norman\Norman Email Protection\mailbox\@Quarantine](#)
 - If the mailstore.mdb file is at or close to 2GB you must:
 - In the Console, go to **System > Services**
 - Stop the MODUSADM service
 - In Windows Explorer, go to the [...mailbox\@Quarantine](#) folder
 - Rename the mailstore.mdb file to mailstore.old (a new one will be recreated)
 - Rename the [...@Quarantine\inbox](#) folder to [...\Quarantine\inbox.old](#)
 - In Services, start the MODUSADM service
 - Email Protection should start processing the backlog

The problem will likely occur again if you continue using an MS Access database

- Using an SQL Server or SQL Server Express database is recommended
- In the interim, if users consent, a work-around is to delete spam instead of sending it to Quarantine
- In the Console, go to **Spam > Preferences > Options**
- Select **Delete the message immediately**

Sieve script mistakenly captures test messages

If test messages are being captured and sent to Quarantine, check that your custom sieve scripts are set up properly.

Do not set your Quarantine to Delete Spam when testing custom sieve scripts. This setting will not effectively determine if the sieve scripts are causing problems.

Third-Party anti-virus blocks messages and locks files

Some customers run third-party anti-virus software on the same machine as Email Protection. This can cause problems on Email Protection versions that provide scanning because the other AV program often locks files as Email Protection attempts to scan them, interfering with message processing. To avoid this situation, ensure that your third-party anti-virus package does not scan the following folders and their sub-folders:

- ...\\Email Protection\\Spool
- ...\\Email Protection\\mailbox\\@Quarantine
- C:\\winnt\\temp

Resolving backlogs in Holding and Domains folders

The ...\\Email Protection\\spool\\holding folder stores messages bound for local and outbound delivery. If there are more than 2,000 messages in this folder, there may be a problem. However, the content of the ...\\Email Protection\\spool\\domains folder is more important as this is what Email Protection uses to coordinate email delivery.

- Check local deliveries:
- Go to the ...\\spool\\domains\\\$local\$ folder to verify the contents
- If there is a large backlog of messages, something is preventing the processing of messages going to the local domains
- In the folder, there should be one of four types of files which are of the same type (envelope files) but the extension of the files indicates what processing has been completed
- **.RCO** files: recently arrived .RCP files that have yet been scheduled for delivery
- **.RCP** files: scheduled for delivery and awaiting processing
- **.LCK** files: locked .RCP files that are in the process of being delivered
- **.DEF** files: deferred files have undergone a delivery attempt and are awaiting retry
- In the Console, go to **System > Mail Delivery** and click **Deliver Now**
- In the ...\\spool\\domains\\\$local\$ folder, press <F5> to refresh the contents of the folder
- If the number of files does not decrease or if it increases after performing a **Deliver Now**, this signifies a problem
- The backlog might be due to communication problems with the authentication server

Possible causes for email backlog

- Authentication failing for local domains
- If your authentication server (AD or LDAP) is down or stops responding, delivery to local mailboxes will fail
 - On the Email Protection server, open a telnet session to the email server to check if it responds to Port 25
 - In the telnet session, open a connection to the Email Protection server on Port 25 and try to send a message to a valid user
 - If the authentication server is unavailable, an error message will appear stating that there is a problem with your user authentication
- Contact Customer Support at support@norman.com

Invirus buildup and/or server freezes at regular intervals

Symptom:

Server seems to freeze at regular intervals making the machine unresponsive for short periods of time (less than a few seconds). In extreme cases, this can cause spool backlogs.

Cause:

Email Protection updates information in the Registry. These write-operations to the Registry are cached in a file called [software.log](#). By default, the OS will purge the cache and write the operations to the Registry hive every 5 seconds for Windows Server 2003 or every 5 minutes Windows 2000 Server.

During these intervals, the system appears to freeze. This behavior is not normal. The root cause is usually a poorly configured RAID controller whereby the Windows operating system is installed with a RAID array.

Solution:

If you use a RAID array for your OS drive with the RAID mode set to **write-through mode** instead of **writeback mode**, by default, the controller only sends an acknowledgement of a disk-write operation after the disk-write has completed. In the example above, no disk-write operations would be acknowledged until the RAID controller has finished purging the cache file and has merged it into the Registry hive. Therefore, it is recommended that the RAID controller on the OS drive be set to use **writeback mode** which sends an acknowledgement before the write-operation is complete. This ensures faster response.

For additional information, please consult the IBM Systems Software Information Center article [Understanding write-cache mode for logical drives](#).

Web application issues

If the Web components are not installed on the same machine as Email Protection, or if the Email Protection machine has more than one NIC, perform the following steps:

WebRoot\Custom.config File

The information contained in this file is required to access the data for WebMonitor.

- If there are multiple NICs on the Email Protection server, you may need to replace "localhost" with the first static IP of the server for the following values:
 - Site
 - WebMailServerAddress
 - MonitoringServerAddress
 - Ensure that the Temp and LogDir values point to the correct location for these files
 - If changes are made to the custom.config file, stop and start the IISAdmin service on the server.

Folder Permissions

Ensure that the appropriate permissions are granted:

Windows Server 2003 and Server 2008

- In Windows Explorer, go to ...\\Program Files\\Norman\\Web
- Right-click on the Web folder and select **Properties > Security**
 - Server 2003: click **Add**
 - Server 2008: click on **Edit > Add**
- At **Select Users or Groups**, click on **Advanced**
- Click on **Find Now**
 - Select **IUSR_Machine** and **Network Service**
 - Click on **OK** (2x)
- For the two new Groups/User Names, give **Modify** permission
 - Click on **Advanced** to replace permission entries on all child objects
 - Click on **OK**
- Stop/start the IIS service

Performance counters

Email Protection supplies a number of Performance Counter objects to help diagnose performance issues, and to help you monitor your system more closely.

To locate the counters, open Windows' Performance Monitor. In the list of Available Counters, you should find each of the following Email Protection services (where applicable): Modusadm, Moduscan, Modusmon, SMTPDS, SMTPRS and Webmailsvr. Expand each item to see its list of available counters.

Appendices

Appendix A: Web applications

WebMonitor

The WebMonitor application provides information about system health and the email statistics. It is preferable to run it on a separate (web) server as it could interfere with Email Protection's performance.

Login

- WebMonitor uses NT authentication
- Your Windows login ID must have permission to access the folder where WebMonitor is located
 - The default folder is `...\Program Files\Norman\Web\Webmonitor`
- To log into WebMonitor, type `/webmonitor/login.aspx` after the server URL

EXAMPLE

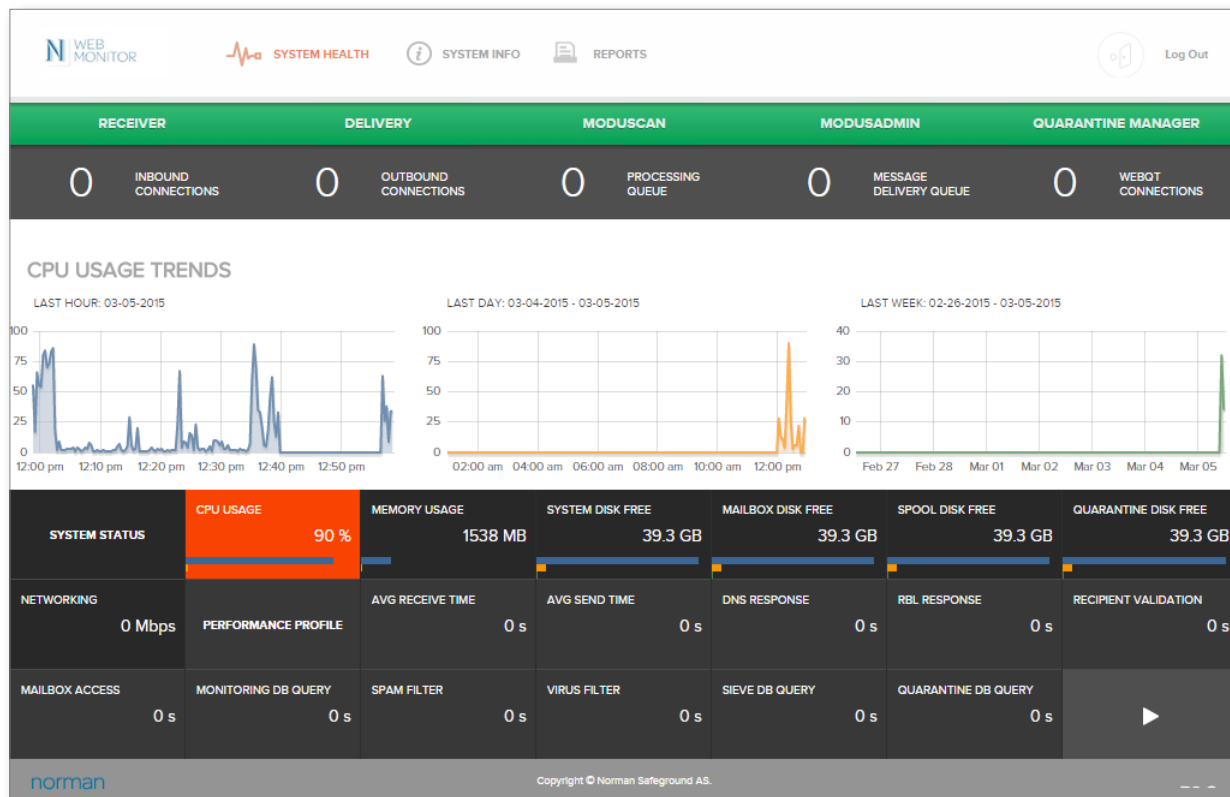
`serveraddress/webmonitor/login.aspx`

System Health

The System Health screen provides the following information:

- **System Status:**
 - Hardware resource usage and networking information
 - Click on a system status cell at the bottom to see performance trend graphs for the last hour, the last day (24 hours) and the last week
 - The blue, yellow and green activity bars in each cell represent the average value taken from the corresponding performance trend graph
- **System Activity:**
 - Inbound and Outbound connections
 - Processing and Message Delivery queues
 - WebQuarantine connections (if installed on a separate server, this will not be available)
 - Shown in the black band above the performance trend graphs
- **Performance Profile:**
 - Average performance rates for messages processed in the last second
 - Click on a performance profile cell at the bottom to see performance trend graphs for the last hour, the last day (24 hours) and the last week
 - The blue, yellow and green activity bars in each cell represent the average value taken from the corresponding performance trend graph
- **System Info:**
 - Version and update information for all systems
- **Service Status:**
 - Indicates the status of the various services

- Shown in the colored band above the black system activity band
- Color changes to identify the service status



Trend Graph Display

There are 3 graphs depicting trends:

- **Last hour:** average readings at 20 second intervals
- **Last day (24hrs):** average readings at 8 minute intervals
- **Last week:** average readings at hourly intervals

Continous Play Button

Click the play button on the bottom right to continously scroll through the various performance trend graphs.

Service Status

The following identifies the service status colors:

- **Green** – the service is functional
- **Orange** – the service is in the process of starting or stopping
- **Red** – the service is stopped

A service may stop and start on its own because of updates. In Windows, go to **Administrative Tools > Services** to verify the status of the service.

Performance Profile

Email Protection measures average component performance for the delivery/processing time of messages passing through the system in the last second. If no messages were processed in the last second, the values will be zero (0).

System Info

The System Info panel provides version and update information for the various system components. Click on a logo for information about each individual component:

- Email Protection: version, license expiry, number of mailboxes, license limit
- SCA: spam engine version and last update
- Avira/Bitdefender: version and last virus engine update
- Windows Server: version, last reboot

Reporting

This feature allows administrators to schedule and view system, domain, and user-level statistical data. The reports can be exported to PDF.

With the exception of the System Overview panel, statistical data presented is for the previous day. However, statistics can be shown for a particular day, week, month or year. The date and time of report generation is displayed with the report title.

System Overview

Clicking the **System Overview** button provides a snapshot of the system activity for the previous day, the previous week and the previous month.

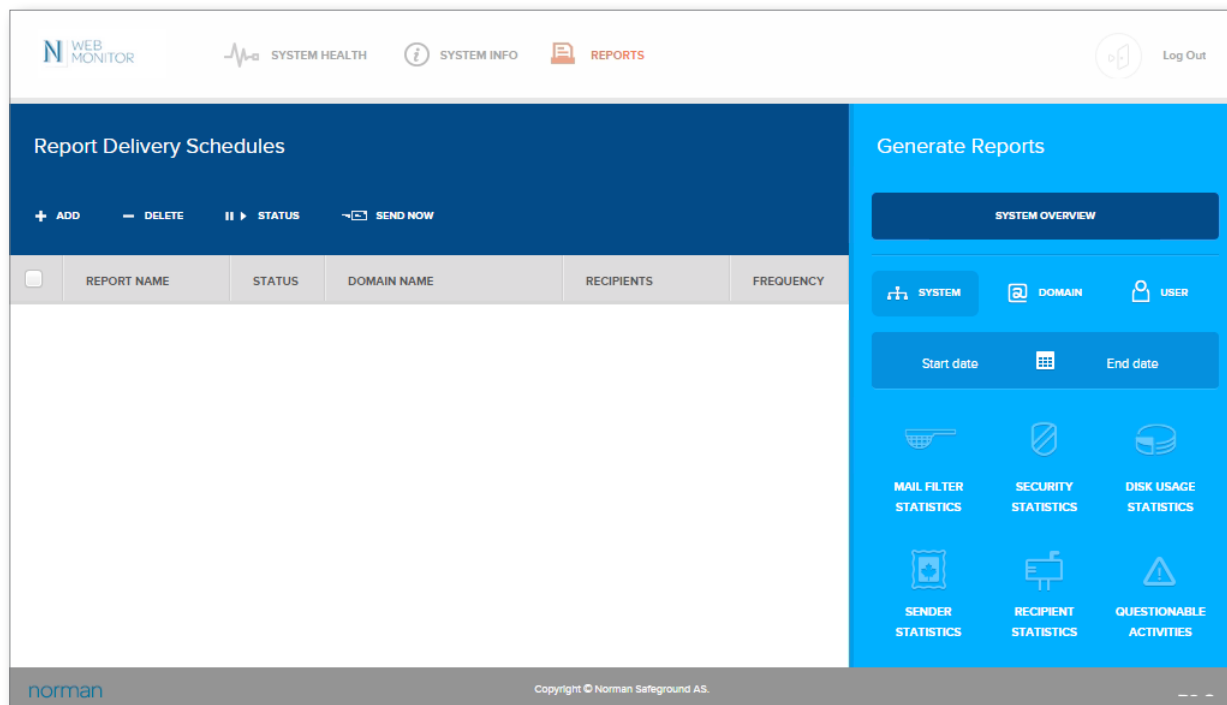
Mail Traffic Spotlight: displays the previous day's most active sender and recipient of legitimate messages, spam and viruses.

Trend Watch: presents a statistical comparison for the past day, week and month for the following measures:

- **Mail Traffic Overview**
Provides information for the total messages scanned with a percentage breakdown for legitimate and blocked messages
- **Blocked Content Breakdown**
Provides blocked content information, in percentages, for messages blocked by each filter
- **Security Overview**
Provides the number of total connections received by Email Protection with a percentage breakdown for connections accepted and connections blocked by all security measures

System

This section provides the following statistical information for the Email Protection system.



Mail Filter Statistics

- Provides a graphical analysis of the messages processed by the system in terms of legitimate email vs. threats, with a further breakdown of the threat types.
- If any of the filters are disabled, the name will appear in the legend but the value will show N/A. If the function is active but there are no results, the value will be 0.

Security Statistics

- Displays the number of connections blocked per security measure enabled in the Console, and the top 10 RBL servers used, to compare their efficacy.

Sender Statistics

- Identifies the top 10 email message senders (local and external).

Recipient Statistics

- Identifies the top 10 local email message recipients.

Disk Usage Statistics

- Displays the top ten local email addresses that use the most disk storage space, for quarantine and mail-box storage.
- Disk usage statistics are compiled daily at 2:00 AM. As such, the reported values may not reflect the actual values at the time the report is requested. Compilation occurs at this time so as not to interfere with other automated processes and because there is likely to be less email traffic. This ensures that the system has sufficient time to count all messages on the server.
- It could take several hours to compile the Disk Usage statistics so be aware of this when scheduling the Disk Usage report.

Questionable Activities

Provides information about questionable email activities and can help identify potential abuse:

Highest Volume Senders (Local)

- Lists the top ten email senders (by email address) for all domains on Email Protection.
- The **Unique Address Count** measures the number of recipients per message.
 - If a message is sent to a mailing list, the list is expanded to count the number of recipients and only applies to legitimate email and spam that is tagged and passed.
- Messages that are quarantined or deleted for spam, F.A. or virus content are counted as one recipient.
- It also can be used to help recognize spamming activity.
 - I.e. if one message is sent to 1,000 recipients, it is likely spam.

Login Authentication Failures by IP (Including Web Logins)

- Lists the top ten failed authentication logins, both internal and external, by IP address
- Includes the authentication type, the number of rejections and the failure rate
- This feature can help to determine if there were attempts to hack into Email Protection

Login Authentication Failures by Email Address (Including Web Logins)

- Lists the top ten failed authentication logins, both internal and external, by email address (i.e. who has attempted to log in)
- Includes the authentication type, the number of rejections and the failure rate
- This feature can help identify if local users are experiencing login problems or determine if there were attacks on Email Protection

Domain

This section provides statistical information for individual domains on Email Protection. Administrators can retrieve the **Mail Filter** and **Disk Usage** statistics by entering the domain name in the Domain field. There is an auto-complete mechanism in place for this.

Users

Provides statistical information for individual users. Administrators can retrieve the **Mail Filter** statistics by entering the complete email address in the **Email** field.

Using the calendar

Click on **Start Date** to select the start date and **End Date** to select the end date.

Exporting reports

All reports can be exported to PDF and Excel.

Scheduling reports

Administrators can schedule Email Protection to email system reports to the addresses of their choice. All system reports can be delivered in both Excel and PDF formats, and on a daily, weekly or monthly basis. Additionally, administrators can use the **Send Now** feature to generate an immediate email message for the scheduled reports.

Add / Edit Schedules CLOSE

Report Type: System ☒ Domain ☐

Report Name: System Overview

Frequency: Day ☐ Week ☒ Month ☐

Receive a daily report for the previous day at: 00:00

Report Format: PDF

Email From:

Email To:

SAVE

When accessing the Report Scheduler for the first time, the error "The system cannot connect with WebMonitor" may appear, along with the System Configuration panel. Copy the URL address from the Address field of the Web browser and paste it into the WebMonitor URL field in the System Configuration. Click on **Save**.

To schedule a report:

- Click Add to open Add/Edit Schedules
- Select the report **type** and **name**
- Set the **frequency** (can be daily, weekly or monthly)
- Set the time to receive the report for the previous day
- Choose the report **format** (PDF or Excel)
- Enter an address to be displayed in the **Email From** field; by default the local postmaster address is used (if configured)
- Enter the recipient email address in the **Email To** field

To delete and change the status of a report:

- Click Delete to delete a selected report
- Click Status to disable/enable scheduled reports

Message Audit

System administrators can audit email messages to get an up-to-date view of email processing. Transactions are displayed in a 1-line summary to provide traceability of who sent the message and when, to whom, whether the message was filtered or delivered, and whether the user opened it.

The screenshot shows the Norman Message Audit interface. At the top, there are navigation tabs: SYSTEM HEALTH, SYSTEM INFO, MESSAGE AUDIT (selected), and REPORTS. Below the tabs is a search bar with a date range selector (Start Date to End Date) and a search icon. The main area displays a table of email transactions with columns: RECEIVED, SENDER, RECIPIENT, SUBJECT, MESSAGE ID, ATTACHMENTS, SIZE, SOURCE, SCAN RESULTS, and STATUS. The table contains several rows of data, including messages from 'js@vircom.com' and 'reporting@...'. A red box highlights a detailed view of a message from 'js@vircom.com' received on 'Thu Nov 28 2013 12:02:51 AM'. The details include a list of actions: 'SMTPRS Moved to \'spool\'invirus', 'MODUSCAN Locked for processing in \'spool\'invirus', 'MODUSCAN Message B0000110639.MSG detected in \'spool\'invirus', 'MODUSCAN Clean', 'MODUSCAN Scanning for forbidden attachments', 'MODUSCAN Scanning for viruses', 'MODUSCAN Clean', 'MODUSCAN Scanning for spam/phishing/foreign', 'MODUSCAN Moved to \'spool\'incoming', 'SMTPDS Message B0000110639.MSG detected in \'spool\'incoming', 'SMTPDS Moved to \'spool\'holding', and 'SMTPDS Delivered to external address js@vircom.com'. To the right of the details is a summary box with fields: Received (11/28/2013 12:02:51 AM), Sender (js@vircom.com), Recipient (js@vircom.com), Subject (Mail Filter Statistics for 11/27/2013), Message ID (B0000110639.msg), Attachments (Mail Filter Statistics for 11/27/2013.pdf), Source (127.0.0.1), Scan Results (Clean), and Status (Delivered). At the bottom of the interface, there are buttons for EXPORT, FORWARD, and RELEASE.

RECEIVED	SENDER	RECIPIENT	SUBJECT	MESSAGE ID	ATTACHMENTS	SIZE	SOURCE	SCAN RESULTS	STATUS
2013-11-28...	js@vircom...	js@vircom...	Mail Filter Statistics for 11/27/2013	B00001106...	Mail Filter ...	106244	127.0.0.1	Clean	Delivered
2013-11-28...	reporting@...	js@qa.lab	System Overview for 11/27/2013	B00001106...	System Ov...	13059	127.0.0.1	Clean	Delivered
2013-11-27...	reporting@...	js@qa.lab	Mail Filter Statistics for 11/17 - 11/23/2013	B00001106...	Mail Filter ...	130123	127.0.0.1	Trusted List	Delivered
2013-11-27...	reporting@...	js@qa.lab	System Overview for 11/26/2013	B00001106...	System Ov...	13059	127.0.0.1	Clean	Scanning
2013-11-27...	reporting@...	js@qa.lab	System Overview for 11/26/2013	B00001106...	System Ov...	13059	127.0.0.1	Clean	Delivered

Thu Nov 28 2013 12:02:51 AM SMTPRS Moved to 'spool'invirus
Thu Nov 28 2013 12:02:51 AM MODUSCAN Locked for processing in 'spool'invirus
Thu Nov 28 2013 12:02:51 AM MODUSCAN Message B0000110639.MSG detected in 'spool'invirus
Thu Nov 28 2013 12:02:51 AM MODUSCAN Clean
Thu Nov 28 2013 12:02:51 AM MODUSCAN Scanning for forbidden attachments
Thu Nov 28 2013 12:02:51 AM MODUSCAN Scanning for viruses
Thu Nov 28 2013 12:02:51 AM MODUSCAN Clean
Thu Nov 28 2013 12:02:51 AM MODUSCAN Scanning for spam/phishing/foreign
Thu Nov 28 2013 12:02:52 AM MODUSCAN Moved to 'spool'incoming
Thu Nov 28 2013 12:02:52 AM SMTPDS Message B0000110639.MSG detected in 'spool'incoming
Thu Nov 28 2013 12:02:52 AM SMTPDS Moved to 'spool'holding
Thu Nov 28 2013 12:02:53 AM SMTPDS Delivered to external address js@vircom.com

Received: 11/28/2013 12:02:51 AM
Sender: js@vircom.com
Recipient: js@vircom.com
Subject: Mail Filter Statistics for 11/27/2013
Message ID: B0000110639.msg
Attachments: Mail Filter Statistics for 11/27/2013.pdf
Source: 127.0.0.1
Scan Results: Clean
Status: Delivered

Searching Messages

The search feature allows you to search for specific messages in the message audit log using various search criteria, including: date sent, sender/recipient address, subject content, scan results, message status, etc.

Search Results

The search results view can be configured to provide up to eight columns of information

- Click on **Settings** on the main screen to select which attributes to present in the search results

The screenshot shows the 'Settings' dialog box for the Message Audit columns. The dialog has a title bar with 'Settings', 'MESSAGE ID', 'ATTACHMENTS', and a 'CLOSE' button. The main content area is titled 'Show Attributes in Message Audit Columns' and contains a list of attributes with checkboxes: Sender, Subject, Size, Scan Results, Source, Received, Attachments, and Status. All checkboxes are checked. At the bottom of the dialog is a 'SAVE' button.

Settings MESSAGE ID ATTACHMENTS CLOSE

Show Attributes in Message Audit Columns

☒ Sender ☒ Source
☒ Subject ☒ Received
☒ Size ☒ Attachments
☒ Scan Results ☒ Status

SAVE

- To view the Message Audit Log details, click on a particular entry
 - In addition to the information available in the search results view, the log detail provides the full transaction history for a particular message

RECEIVED	SENDER	RECIPIENT	SUBJECT	MESSAGE ID	ATTACHMENTS	SIZE	SOURCE	SCAN RESULTS	STATUS
2013-11-28...	js@vircom...	js@vircom...	Mail Filter Statistics for 11/27/2013	B00001106...	Mail Filter ...	106244	127.0.0.1	Clean	Delivered
2013-11-28...	reporting@...	js@qa.lab	System Overview for 11/27/2013	B00001106...	System Ov...	13059	127.0.0.1	Clean	Delivered
2013-11-27...	reporting@...	js@qa.lab	Mail Filter Statistics for 11/17 - 11/23/2013	B00001106...	Mail Filter ...	130123	127.0.0.1	Trusted List	Delivered
2013-11-27...	reporting@...	js@qa.lab	System Overview for 11/26/2013	B00001106...	System Ov...	13059	127.0.0.1	Clean	Scanning
2013-11-27...	reporting@...	js@qa.lab	System Overview for 11/26/2013	B00001106...	System Ov...	13059	127.0.0.1	Clean	Delivered

Thu Nov 28 2013 12:02:51 AM SMTPRS Moved to \spool\inivirus
Thu Nov 28 2013 12:02:51 AM MODUSCAN Locked for processing in \spool\inivirus
Thu Nov 28 2013 12:02:51 AM MODUSCAN Message B0000110639.MSG detected in \spool\inivirus
Thu Nov 28 2013 12:02:51 AM MODUSCAN Clean
Thu Nov 28 2013 12:02:51 AM MODUSCAN Scanning for forbidden attachments
Thu Nov 28 2013 12:02:51 AM MODUSCAN Scanning for viruses
Thu Nov 28 2013 12:02:51 AM MODUSCAN Clean
Thu Nov 28 2013 12:02:51 AM MODUSCAN Scanning for spam/phishing/foreign
Thu Nov 28 2013 12:02:52 AM MODUSCAN Moved to \spool\incoming
Thu Nov 28 2013 12:02:52 AM SMTPDS Message B0000110639.MSG detected in \spool\incoming
Thu Nov 28 2013 12:02:52 AM SMTPDS Moved to \spool\holding
Thu Nov 28 2013 12:02:53 AM SMTPDS Delivered to external address js@vircom.com

EXPORT **FORWARD** **RELEASE**

Received	11/28/2013 12:02:51 AM
Sender	js@vircom.com
Recipient	js@qa.lab
Subject	Mail Filter Statistics for 11/27/2013
Message ID	B0000110639.msg
Attachments	Mail Filter Statistics for 11/27/2013.pdf
Source	127.0.0.1
Scan Results	Clean
Status	Delivered

- Click on **Export** to export the log detail for a particular message to a HTML or text file
- The file can be opened in a Web browser or saved to any location
- Click on **Forward** to forward the log
 - The message is sent from the postmaster account
- Click on **Release** to release blocked messages to their destined recipients

WebAdmin

The WebAdmin application provides Web access to the administrative functions of Email Protection. Mirroring the Domain and User properties of the Administrative Console, IT administrators can use it to manage Email Protection remotely or grant access to domain administrators to manage their own user settings. This can be useful for organizations that host multiple domains.

The WebAdmin feature is not available for unlimited user licenses. In addition, because the functions in WebAdmin are identical to those in the Console, the information contained in this section is limited. Complete details can be found throughout this guide.

Login

To log into WebAdmin, type /webadmin after the server URL

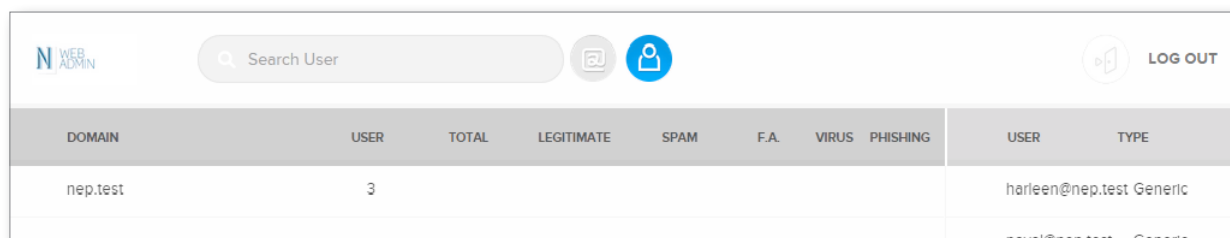
EXAMPLE serveraddress/webadmin

WebAdmin was developed for system and domain administrators. Access should not be given to end users.

Before users can access WebAdmin, they must be granted permission. For details, see "WebAdmin Privileges" on page 81.

Main Page

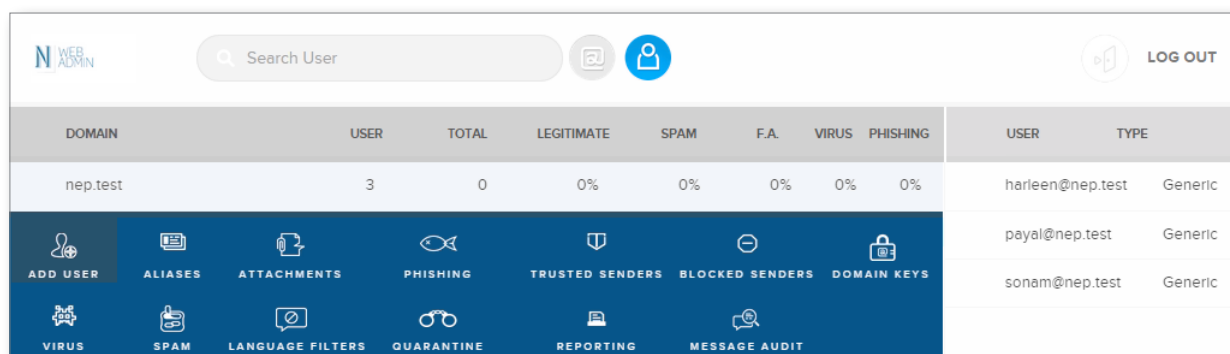
The main page provides access to the domain view, user view and configuration options. It also provides a weekly summary of the message statistics for your domains and users. The left side displays the domain view and the right side displays the user view.



DOMAIN	USER	TOTAL	LEGITIMATE	SPAM	F.A.	VIRUS	PHISHING	USER	TYPE
nep.test	3							harleen@nep.test	Generic
								payal@nep.test	Generic

Domain View

The Domain view provides access to the following configuration panels. All settings available in the Administration Console are also available here. To access the configuration panels click on a domain name:



DOMAIN	USER	TOTAL	LEGITIMATE	SPAM	F.A.	VIRUS	PHISHING	USER	TYPE
nep.test	3	0	0%	0%	0%	0%	0%	harleen@nep.test	Generic
								payal@nep.test	Generic
								sonam@nep.test	Generic

- **Add User:** add a new user mailbox for the domain
- **Aliases:** manage aliases for the domain
- **Attachments:** override the system defaults for processing messages containing forbidden attachments
- **Phishing:** override the system defaults for processing phishing messages
- **Trusted Senders:** manage the trusted senders list for the domain
- **Blocked Senders:** manage the blocked senders list for the domain
- **Domain Keys:** view the domain key and enable DKIM for outbound messages
- **Virus:** override the system defaults for virus handling
- **Spam:** override the system defaults for processing spam messages
- **Language Filters:** override the system defaults for processing messages with foreign language content and configuring blocked languages
- **Quarantine:** manage (delete and release) quarantined mail by category: spam, attachments, phishing and viruses
- **Reporting:** override the system defaults for the Quarantine Report frequency, content and settings
- **Message Audit:** override the system defaults for message audit logging

N

WEB ADMIN

Search User

LOG OUT

DOMAIN	USER	USER	TYPE	TOTAL	LEGITIMATE	SPAM	F.A.	VIRUS	PHISHING
nep.test	3	harleen@nep.test	Generic	0	0%	0%	0%	0%	0%
		<div><div><div><div></div><div>DELETE USER</div></div><div><div></div><div>ALIASES</div></div><div><div></div><div>ATTACHMENTS</div></div><div><div></div><div>PHISHING</div></div><div><div></div><div>TRUSTED SENDERS</div></div><div><div></div><div>BLOCKED SENDERS</div></div><div><div></div><div>VIRUS</div></div><div><div></div><div>SPAM</div></div><div><div></div><div>LANGUAGE FILTERS</div></div><div><div></div><div>QUARANTINE</div></div><div><div></div><div>REPORTING</div></div><div><div></div><div>MESSAGE AUDIT</div></div></div></div>							
		payal@nep.test	Generic						
		sonam@nep.test	Generic						

- **Delete User:** delete the user mailbox
- **Aliases:** manage aliases for the user mailbox
- **Attachments:** override the domain defaults for processing messages containing forbidden attachments
- **Phishing:** override the domain defaults for processing phishing messages
- **Trusted Senders:** manage the trusted senders list for the user mailbox
- **Blocked Senders:** manage the blocked senders list for the user mailbox
- **Virus:** override the domain defaults for virus handling
- **Spam:** override the domain defaults for processing spam messages
- **Language Filters:** override the domain defaults for processing messages with foreign language content and configuring blocked languages
- **Quarantine:** manage (delete and release) quarantined mail by category: spam, attachments, phishing and viruses
- **Reporting:** override the domain defaults for the Quarantine Report frequency, content and settings
- **Message Audit:** override the domain defaults for message audit logging

Appendix B: Formal command syntax

The SMTPDS and SMTPRS services may be controlled from a command line by using command-line arguments.

The following options apply for both SMTPRS and SMTPDS.

Syntax

```
smtprs [-remove | -install] [-version]  
      [-ipaddress] [-status] [-start]  
      [-stop]
```

Options

- **-install**: adds the SMTPRS server to the list of installed services
- **-remove**: removes the SMTPRS server from the list of installed services, and will delete the SMTPRS server-specific configuration information from the Registry
- **-version**: reports the version number of SMTPRS server
- **-ipaddress**: reports the IP addresses used for SMTPRS connections
- **-status**: reports the current status of the SMTPRS server, i.e. whether or not it is running
- **-start**: starts the SMTPRS server
- **-stop**: stops the SMTPRS server

Appendix C: Interacting with Exchange

This section explains how Email Protection interacts with Exchange and Active Directory.

Disabled user objects:

- When an account is disabled in Active Directory, it can no longer access the server to use server and network resources.
- Mailbox attributes assigned to the disabled account may be kept.
- When Email Protection performs a lookup on an AD object, it does not check the status of the account (enabled or disabled).
 - It looks for specific flags to determine if the user's mailbox is enabled.
 - This ensures that, if Exchange is routing email for the object, Email Protection creates an account for the object and route email to the Exchange server for processing.

Secure LDAP with AD:

- When Email Protection performs LDAP authentication over a TSL secured link with a Domain Controller, AD only accepts User DN values in the form of username@domain.local.
 - When Email Protection searches for account information while performing user authentication, it uses the user principal name as the default authentication account.
- If the user principal name is not used, you will need to fill in this account.

Forwarded accounts

- When an email enabled account in Active Directory specifies an external email domain in its primary SMTP address attribute, Exchange re-routes the message to the user's specified external account

EXAMPLE

- Local domain = mymaildomain.com
- Domain configured in Email Protection = mymaildomain.com
- Local user's primary email attribute = user1@mymaildomain.com
- External user's primary email attribute value = user2@hismaildomain.com
- External user's secondary email attribute value = user2@mymaildomain.com
- If mail is sent to user1, the message is processed normally and delivered to user1's mailbox
- If mail is sent to user2, the external account is added as an alias to the account hosted in Email Protection so that mail is delivered to user2's mailbox
- Users with external accounts cannot log into WebQuarantine with their alias addresses
- They can only log into WebQuarantine with an account entered in the users directory

Appendix D: Processing Trusted and Blocked senders lists

This section provides information about the behaviors for the Trusted and Blocked Senders lists, including the way various security checks are processed:

Trusted and Blocked Senders lists can be created at the system, domain and user levels. The following is the sequence of events that occurs once Email Protection receives a message:

- Check the connection limits (total connections & maximum connection rate and the total simultaneous connections from the same IP address & simultaneous connection rate from the same IP address)
 - Bypass this test if a host is in the trusted list or in transparent mode (i.e. when Email Protection hides a source IP address)
- Check for required authentication
 - If SMTP authentication is enabled and is forced and the host is in the list of forced authentication IP addresses, authentication is required ([Security > SMTP Security](#))
- Reject all connections from hosts in the [Reject all incoming mail from](#) list ([Security > Connections](#))
- Simultaneously start reverse and RBL lookups if the following conditions are met:
 - Reverse DNS or RBL lookup or both are enabled ([Security > Sender Reputation](#) and [Real-Time Blacklist](#))
 - The host is not in the trusted list
 - RBL lookup is enabled and the host is not in the IP address exclusion list for RBL lookups
 - The connection does not come from one of the routed IP addresses in Email Protection, and Email Protection is configured to hide a protected server (i.e. placed in front of the email server)
- Place the RBL lookup result in the envelope of the received message
- If reverse DNS is enabled and fails, the connection is refused with the default message "This system is configured to reject email from host [IP address]. DNS reverse lookup failed."
- If the host is found on an RBL, the envelope will contain the header X-Modus-RBL will be set to IP=Blacklisted. Furthermore, if [Reject connection immediately if the host is blacklisted](#) is enabled ([Security > Real-Time Blacklist](#)) and [Postpone the rejection until authentication](#) is disabled ([Security > Sender Reputation](#)), the connection will be rejected.
- If the host is found on an RBL and [Postpone the rejection until authentication](#) is enabled, the decision will be delayed until the user can be authenticated
- At the email From: command, if reverse DNS is enabled and fails, or if RBL lookup is enabled and fails and Email Protection is not configured to reject the connection immediately if the host is blacklisted, the connection is rejected
- After the Mail From: command, Email Protection checks for SPF support and performs a [Look up for SMTP host in the real-time whitelist servers](#), if enabled ([Security > Sender Reputation](#))
- At the scanning stage, Email Protection does not scan internally-generated messages or messages from IP addresses in the list of trusted addresses ([Security > Trusted Address List > Scanning Trusted Address](#))
- If the message contains an attachment greater than the configured limit, Email Protection does not scan it ([Rules > Performance > Attachment Size Verification](#))
- Email Protection does not scan messages from SMTP authenticated users (this is configurable) but it always scans for forbidden attachments and viruses
- Checks the scan properties for each recipient (e.g. spam, virus & attachment scanning levels)
- Checks the Trusted and Blocked Senders lists for each recipient

Glossary

Address/Email Harvesting: The process of obtaining lists of email addresses for use in bulk email or spam.

Alias: An alias is an email address that forwards all email it receives to another email account.

Content Filtering: Spam scanning plain text for key phrases and the percentage of HTML, images and other indications that the message is spam.

Denial of Service (DoS): An attempt to make a computer resource unavailable to its intended users. Considered an Internet crime.

Dictionary Attack: A system of combining letters and numbers in an attempt to find active email addresses. Any addresses to which messages are delivered, as opposed to being bounced back, are legitimate.

Directory Service: A network service that identifies all resources on a network and makes them accessible to users and applications. The software stores and organizes information about a computer network's users and network shares and allows network administrators to manage users' access to the shares. Resources include email addresses, computers and peripheral devices. There are a number of directory services that are used, including Active Directory and LDAP.

DNSBL: DNS Blackhole List or Blacklist, also known as RBL (Real-time Black List). It is a means by which an Internet site may publish a list of IP addresses, in a format which can be easily queried by computer programs on the Internet. Some organizations offer a free service that provides a list of known spammers, updated in real-time.

ESMTP: Extended SMTP. See SMTP.

False Negative: A false negative occurs when spam is not recognized by a spam solution and delivered to a email inbox.

False Positive: A false positive occurs when legitimate email is incorrectly recognized by a spam solution and not delivered to a email inbox.

Filter Scripting: Advanced filtering logic method to block many or all spam tactics.

Fingerprinting: Smart file type detection. A technology that scans email attachments in search of forbidden file formats (e.g. *.exe) in order to prevent them from concealed with modified file extensions.

Headers: The top portion of a message that contains the sender's name, date the message was sent, recipients' names, title, routing details, message priority, and other information.

LDAP: Lightweight Directory Access Protocol. Standard protocol for the exchange of directory entries between servers.

LDIF: LDAP Data Interchange Format. The format used by an LDAP server when returning information for LDAP requests.

MIB: Management Information Base. A MIB is a file that contains descriptions about the characteristics of a Email Protection Server (or any other managed device on a network for which a MIB has been created). The characteristics described in the MIB are the functional elements for the Email Protection Server which can be monitored using SNMP software.

ODBC: Open Database Connectivity. ODBC is an application programming interface (API) used to access third-party databases.

Open Proxy: A proxy that allows computers to use it to make connections to services on their behalf, whether they would normally have permission to access the service or not.

Open Relay: An SMTP (mail) server configured in such a way that it allows anyone on the Internet to relay (i.e. send) email through it. Often open to attack and hijacked to send large amounts of spam.

Phishing: A scam that uses spam to deceive people into disclosing their credit card numbers, bank account information, passwords and other sensitive information. Phishers often masquerade as trustworthy or well-known businesses.

POP3: Post Office Protocol 3. A standard email protocol for authenticating and retrieving email over the Internet. Unlike IMAP (where email resides on the server), POP3 moves messages from the server to the users' computers.

Quarantine: email that has been blocked because of suspicious content, viruses or forbidden attachments.

Reverse DNS: A process to determine the host name associated with a given IP address. This feature ensures that users are from legitimate domains.

Sieve: Simple scripting language used to filter email. One of the more powerful features of sieve is filtering spam. Sieve is defined in RFC3028.

SMTP: Simple Mail Transport Protocol. The protocol used to deliver email to its destination.

SNMP: Simple Network Management Protocol. SNMP is part of the TCP/IP protocol. SNMP applications run in a network management station (NMS) and issue queries to gather information about the status, configuration, and performance of external network devices.

Spam: Unsolicited, bulk email; also known as junk mail.

SPF: Sender Policy Framework. SPF helps to prevent return-path address forgery and makes it easier to identify spoofed addresses. For more information, go to www.openspf.net or RFC 4408.

Spoof: In the context of network security, a spoofing attack is a situation in which a person or program successfully masquerades as another by falsifying data. With phishing, a legitimate Web page (such as a bank's) is reproduced in look and feel by the phisher. The intent is to trick users into thinking that they are connected to a trusted site so that they will enter personal information. The phisher then harvests that information.

SURBL: Spam URI Real-time Block Lists. A SURBL detects spam messages based on message body URIs instead of the spam senders. They allow you to block messages that have spam hosts mentioned in the message bodies. For more information, go to www.surbl.org.

URI: A string of characters used to identify or name a resource. The main purpose is to enable interaction with representations of the resource over the Internet using specific protocols.

URL: Universal or Uniform Resource Locator. An Internet address used by Web browsers to access a specific site or a document (resource).

Virus: Any piece of code that replicates and executes itself. Viruses usually deliver a piece of malicious code that carries out a destructive operation on the host machine.

Offices

General info	www.norman.com
Norway	www.norman.com/no
Denmark	www.norman.com/dk
France	www.norman.com/fr
Germany	www.norman.com/de
Italy	www.norman.com/it
Netherlands	www.norman.com/nl
Norway	www.norman.com/no
Spain	www.norman.com/es
Sweden	www.norman.com/sv
Switzerland	www.norman.com/ch
United Kingdom	www.norman.com/uk

CONTACT DETAILS

AVG Technologies Norway AS | PO box 43, 1324 Lysaker, Norway | Office address: Strandveien 15 Lysaker
Tel: 67 10 97 00 | E-mail: sales.nordics@avg.com | www.norman.com



November 2014 Norman was acquired by AVG Technologies.
We have teamed up to develop the best security software for
businesses and consumers.

